Academy of Applied Technology LLC d/b/a Applied Technology Academy

Learning Catalog

A customer service oriented technical education academy designed to service the needs of individuals, corporations, the military and career changers alike, who desire to improve upon their existing knowledge and skills or for those who desire to initially endeavor upon developing their computer and project management skills.

Licensed by the Commission for Independent Education, Florida Department of Education.
Additional information regarding this institution may be obtained by contacting the Commission at: 325 West Gaines Street, Suite 1414, Tallahassee, FL 32399-0400
Toll-free telephone number 888 (224-6684).

"CERTIFIED TRUE AND CORRECT IN CONTENT AND POLICY"
Official Signatory:
Name: Lynn Fisher

Signature: _____

Date of Publication:
January 1, 2023
Volume 3

1992 Lewis Turner Blvd., Ste. 131, Fort Walton Beach, FL 32547
(800) 674-3550

Table of Contents

- Preparation for Python Programming Professional
- Preparation for Cisco Certified Network Administrator
- Preparation for Cisco Certified Network Enterprise Professional
- Preparation for Microsoft Modern Desktop Administrator Associate
- Preparation for Microsoft 365 and Azure Security Administrator Associate
- Preparation for Microsoft Enterprise Administrator Expert
- Preparation for ITIL Foundations
- Preparation for Project Management and Six Sigma Professional
- Preparation for Certified Six Sigma Green Belt Professional
- Preparation for Adobe Certified Associate – To be retired

Page 163-165 Program Tuition and Fee Payment Schedules

General Information

HISTORY
In 2008, Tech Strategies International incorporated to serve government and military clients with computer, networking and cybersecurity training via Instructor-Led classes.
In August of 2019, the company re-branded and incorporated as Academy of Applied Technology d/b/a Applied Technology Academy with the intent to broaden its student base to include career changers, individual veterans, and Career Source participants in addition to its current corporate and government clients.

The company offers expertise in:

- » Corporate Training
- » Career Training
- » Applications Training
- » Technical Certifications
- » Customized Training Solutions for Businesses, Individuals, Government, & Military

PHILOSOPHY
Applied Technology Academy believes that any person willing to apply themselves to the study of computers can benefit from the training offered by the school. The school provides training from entry level to those areas needed to become a Cybersecurity Professional. The school provides hands on training, textbooks, labs, and instruction, which have been certified, by Microsoft, CompTIA, Cisco Press, EC-Council, and other vendors in order to prepare the student for the final examination and certification.

PURPOSE
The purpose of the institutions is to provide computer and business skills related training and contract training. The school strives to provide quality education and to produce competent graduates who can succeed at their next level of endeavor in an ever-changing richly diverse society.

The school provides a well-balanced curriculum in an environment conducive to learning and delivered by a highly qualified staff with a commitment to excellence. The school recognizes its responsibility to assist students in the achievement of their success.

OWNERSHIP
Academy of Applied Technology LLC D/B/A Applied Technology Academy, a limited liability company, formed under the laws of the State of Florida. This entity is a Single Member LLC.
Owner: Lynn Fisher
Corporate Address: Applied Technology Academy, 2151 W. Hillsboro Blvd., Suite 210, Deerfield Beach, FL 33442

GOVERNING BODY

The principal corporate office of the LLC is located at 2151 W. Hillsboro Blvd., Suite 210, Deerfield Beach, FL 33442 with our training facility located at 1992 Lewis Turner Blvd., Ste. 131, Fort Walton Beach, FL 32547.

ADMINISTRATION:
Owner and President: Lynn Fisher - Fulltime
Training Operations Manager: Open Position – Fulltime
Client Services Education Consultant and Student Navigator: Liz Pernaselci - Fulltime
Bookkeeper: Kari Litoborski – Part Time Contractor

FACULTY:

Faculty Member Name	Classes/Programs Taught	Certificates
Jerry Chaney	CompTIA A+ CompTIA Network+ CompTIA Security+ CompTIA Project+ Microsoft Project Microsoft Excel 1 & 2	Instructor is certified to teach all courses listed under the Programs Taught section by appropriate vendors as noted below: 1. CompTIA A+ 2. CompTIA Network+ 3. CompTIA Security+ 4. CompTIA CIOS 5. CompTIA CSIS 6. Microsoft Certified Technology Professional 7. Microsoft Certified Professional 8. Microsoft Specialist Project
Royal Harrell	CompTIA Security+ CompTIA Linux+ CompTIA CySA+ CompTIA CASP+ CompTIA Pentest+ CompTIA CTT+ CompTIA Cloud+ CompTIA A+ ISC^2 CAP ISC^2 CISSP ISC^2 CISSP-ISSEP ISC^2 CISSP-ISSAP ISC^2 CSSP ISC^2 CSSLP	AA in Electronics from Victor Valley College BS in IT Management from the University of Maryland MS in Security and DBMS from the University of Maryland Instructor is certified to teach all courses listed under the Programs Taught section by appropriate vendors as noted below:

Royal Harrell	ISACA CISA ISACA CISM EC-Council LPT EC-Council CEH EC-Council ECSA EC-Council CHFI EC-Council CND Offensive Security PWK	1. CompTIA Security+ 2. CompTIA Linux+ 3. CompTIA CySA+ 4. CompTIA CASP+ 5. CompTIA Pentest+ 6. CompTIA CTT+ 7. CompTIA Cloud+ 8. CompTIA A+ 9. ISC^2 CAP 10. ISC^2 CISSP 11. ISC^2 CISSP-ISSEP 12. ISC^2 CISSP-ISSAP 13. ISC^2 CSSP 14. ISC^2 CSSLP 15. ISACA CISA 16. ISACA CISM 17. EC-Council LPT 18. EC-Council CEH 19. EC-Council ECSA 20. EC-Council CHFI 21. EC-Council CND 22. PWK-OSCP
Wayne Brantley	PMP Agile Agile SCRUM ITIL Foundations CSM	BS in Education from the University of Southern MS MS in Education from the University of Southern MS Instructor is certified to teach all courses listed under the Programs Taught section by appropriate vendors as noted below: 1. Project Management Professional (PMP) 2. Project Management Institute Agile Certified Practitioner (PMI-ACP) 3. Certified Scrum Master (CSM) 4. Advanced Certified Scrum Product Owner (A-CSPO) 5. ITIL Foundations
Dr. Brian Salk	PMP ITIL Foundations Leadership Courses	BSA in Marketing from the University of Michigan

Dr. Brian Salk	Management Courses	MA in Education from the University of Michigan MA in Human and Organizational Systems from Fielding Graduate University PhD in Human and Organizational Systems from Fielding Graduate University Instructor is certified to teach all courses listed under the Programs Taught section by appropriate vendors as noted below: 1. Project Management Professional (PMP) 2. Project Management Institute Agile Certified Practitioner (PMI-ACP) 3. ITIL Foundations
Robert Fleming	CompTIA Security+ Cisco CCENT Cisco CCNA Routing and Switching Cisco CCNA Security Cisco CCSI	BS in Business from the University of South Florida Instructor is certified to teach all courses listed under the Programs Taught section by appropriate vendors as noted below: 1. CompTIA Security+ 2. Cisco CCENT 3. Cisco CCNA Routing and Switching 4. Cisco CCNA Security 5. Cisco CCSI
Eric Reed	ISC^2 CISSP CompTIA Network+ CompTIA Security+ EC-Council CND EC-Council CEH and CEH Practical EC-Council CHFI EC-Council ECSA	Instructor is certified to teach all courses listed under the Programs Taught section by appropriate vendors as noted below: 1. ISC^2 CISSP 2. CompTIA Network+ 3. CompTIA Security+

Eric Reed	EC-Council CCISO	4. EC-Council CND 5. EC-Council CEH and CEH Practical 6. EC-Council CHFI 7. EC-Council ECSA 8. EC-Council CCISO
John Chris Pope	Microsoft Certified Trainer (MCT) CompTIA A+ CompTIA Network+ CompTIA Security+ CompTIA CySA+ CompTIA Linux+	Instructor is certified to teach all courses listed under the Programs Taught section by appropriate vendors as noted below: 1. Microsoft Certified Trainer (MCT) 2. CompTIA A+ 3. CompTIA Network+ 4. CompTIA Security+ 5. CompTIA CySA+ 6. CompTIA Linux+
Brian Macon	Six Sigma Agile SCRUM CCM CCIM	Instructor is certified to teach all courses listed under the Programs Taught section by appropriate vendors as noted below: 1. Lean Six Sigma Master Black Belt (LSSMBB) 2. Certified Kaizen Facilitator (CKF) 3. Project Management – Lean Process Certified (PM-LPC) 4. Six Sigma Champion Certified (SSCC) 5. 5SC Certified (5SC) 6. Lean Six Sigma Black Belt – Healthcare (LBBH) 7. Certified Continuous Improvement Manager (CCIM) 8. Certified Conflict Manager (CCM)
Juan Oquendo	Adobe Creative Cloud CompTIA Project+ CompTIA Server+ Project Management Professional	Instructor is certified to teach all courses listed under the Programs Taught section by appropriate vendors as noted below:

Juan Oquendo		1. Project Management Professional (PMP) 2. Microsoft Office Specialist 3. CompTIA TTA 4. CompTIA Project+ 5. CompTIA Server+ 6. Adobe Certified Educator
John McCardle	Microsoft Python Python Programming Linux+ CompTIA Network+ CompTIA Linux+ EC-Council CEH EC-Council CHFI Microsoft MCSE	BA in Russian Studies from the University of South Florida MS in Intelligence Studies from the University of South Florida Instructor is certified to teach all courses listed under the Programs Taught section by appropriate vendors as noted below: 1. CompTIA Network+ 2. CompTIA Linux+ 3. EC-Council CEH 4. EC-Council CHFI 5. Microsoft MCSE 6. Microsoft Tech Assoc. Python 7. CCNA
Andrew Palladino	Cisco CCNA Cisco ENCOR Cisco ENARI Cisco SCOR Cisco SISE Cisco SVPN Cisco SESA Cisco SWSA Cisco SSNGFW Cisco SSFIPS CompTIA A+ CompTIA Network+ CompTIA Security+ Microsoft Python CyberSecure Coder	BA in Experimental Psychology from the University of Connecticut Instructor is certified to teach all courses listed under the Programs taught section by appropriate vendors as noted below: 1. Cisco CCNA 2. Cisco ENCOR 3. Cisco ENARI 4. Cisco SCOR 5. Cisco SISE 6. Cisco SVPN 7. Cisco SESA 8. Cisco SWSA

Andrew Palladino		9. Cisco SSNGFW 10. Cisco SSFIPS 11. CompTIA A+ 12. CompTIA Network+ 13. CompTIA Security+ 14. CompTIA CTT+ 15. Microsoft Python
David K. Slater	CompTIA Network+ CompTIA Security_ CompTIA CASP+ CompTIA CySA+ CyberSec First Responder	MS, Computer Information Systems, University of Phoenix, 2006 Instructor is certified to teach all courses listed under the Programs taught section by appropriate vendors as noted below: 1. CompTIA Network+ 2. CompTIA Security_ 3. CompTIA CASP+ 4. CompTIA CySA+ 5. CyberSec First Responder

Applied Technology Academy maintains adequate staffing levels to teach all the classes that we run at any of Fort Walton Beach location or via Distance Learning classes. If a class fills up and is at maximum capacity, then we will immediately schedule a new class as needed with enough time between them in order to ensure that classes do not run with more students than our maximum capacity, and also to ensure that we always are able to have instructors available to teach any class that is taking place.

DESCRIPTION OF SCHOOL FACILITIES

The Fort Walton Beach campus is located in a 21,765 square foot facility located at 1992 Lewis Turner Boulevard, Suite 131, Fort Walton Beach, FL 32547. Our school consists of a leased 25 student classroom that is approximately 833 square feet, break room, business office and testing facility that is approximately 170 square feet in this commercial multi-tenant building by the name of Workspace Suites. The classroom is used for the study of computer related subjects equipped with current computer hardware needed for classes and has a 25-student capacity. A library with a dictionary and thesaurus is located at the back of the classroom. There is one computer and monitor per person, video and overhead projector and full wall white board for visual aids. We utilize videoconferencing software to deliver hybrid distance learning courses from our Fort Walton Beach facility as well. The testing facility is a private Pearson VUE Authorized Test Center.

We also house a full mobile laptop classroom and a mobile Pearson VUE Test Center in our management office for mobile classes at local military bases and corporations. These are typically utilized for contract training courses.

APPROVAL FROM NON-GOVERNMENTAL AGENCIES

CompTIA Authorized Training Partner (2008)
Certified that we are technically sound to deliver A+, Network+, Security+, Linux+, Project+, Server+, CySA+, Pentest+ and CASP+ CompTIA certification programs

EC-Council Accredited Training Center (2014)
Certifies that we meet EC-Council's rigorous requirements to deliver all of their certification courses. We have been awarded their Academia Circle of Excellence Award 3 years running.

Microsoft Academy Partner (2014)
Allows us to deliver all Microsoft Academy certification training and to maintain multiple MCTs

Offensive Security Platinum Partner and Learning Partner (2021)
Allows us to deliver Authorized Instructor-Led Offensive Security training nationwide.

APPROVAL FROM GOVERNMENTAL AGENCIES

- Verified Florida Woman Owned Small Business
- SBA Certified Woman Owned Small Business

AMERICANS WITH DISABILITIES ACT
Applied Technology Academy is in a facility that meets ADA requirements. Special single occupancy restrooms are available for special needs. Elevators include Braille raised letters on their control panels. Control panels are lowered to accommodate wheelchair height. The

classroom and laboratory PC stations are at a desk height to accommodate wheelchair access. Questions relative to ADA accessibility should be directed to the Operations Manager who can be reached during the Hours of 9 AM thru 5 PM Monday thru Friday.

SMOKE FREE SCHOOL POLICY

To protect and enhance our indoor air quality and to contribute to the health and well-being of all employees and students, Applied Technology Academy is an entirely smoke free institution. The use of tobacco and smoking products, including chewing tobacco and using electronic cigarettes (E-cigarettes) is banned from our facilities.

Smoking is prohibited in all of the enclosed areas within the school, without exception. This includes common work areas, classrooms, conference and meeting rooms, private offices, hallways, the lobby, the break rooms and all other enclosed facilities.

Not complying with this policy may be grounds for dismissal and/or termination.

HOURS OF OPERATION

The business office is open from 9:00 am to 5:00 pm EST Monday through Friday. Registration will be conducted from 9:00 am to 5:30 pm EST Monday through Friday.

Classes are in session:
Monday through Friday 8:00 to 4:00 pm (CST/EST) and 6:00 to 9:30 pm (CST/EST)

CLASS SCHEDULE

Applied Technology Academy is very flexible in scheduling students. Applied Technology Academy has ongoing enrollments that start every month. All courses are determined by Vendor standards.

Full Time Students:
Monday through Friday: 8:00 am to 4:00 pm

Part-Time Students:
Monday through Thursday: 6:00 pm to 9:30 pm, 6:00 pm to 10:00 pm or 7:00 pm -11:00 pm. Some Saturdays allowed for make-up 8:00am – 4:00pm.

When an unexpected closure occurs due to extraordinary conditions such as inclement weather, students will be notified as soon as possible by phone and/or radio, and/or TV who provide closure information as a public service.

Classes are not held on the following holidays:

HOLIDAYS

Classes will not be held on the following holidays:

New Year's Day
Memorial Day
Independence Day
Labor Day
Thanksgiving Day
Christmas Day

ADMISSIONS

POLICY STATEMENT
The school does not discriminate regarding race, color, creed and/or religion. The training offered by the school is also recommended to handicapped persons who are unable to undertake strenuous vocations or lack the mobility required by other occupations.

ADMISSION REQUIREMENTS
An applicant must have a high school diploma or equivalency diploma with the willingness to learn; and a working knowledge of computers would be greatly appreciated. We also screen our students to make sure they will be successful with our program. A prospective student requesting admission may be asked to take entry-level class(es) before entering into a program. There would be no testing on these entry-level classes that would keep the applicant from entering the program. If the applicant did not have even basic knowledge of entry-level classes, which may be prerequisites for a program, applicant may be required to take the entry-level class(es) before entering the program. Students must show that they have a basic knowledge of the program during their interview prior to enrollment.

A student wishing to apply for enrollment may attend a (one day PC class) session prior to entering the program at no cost. Students are encouraged to attend the class to determine his or her level of commitment and financial obligation.

Each student is assigned a Student Navigator that interviews the student prior to any program. The Student Navigator will continue to monitor the student as well as counsel them through each program. Each Student Navigator is trained and tested to council students proficiently in specific programs that the school offers.

ACCEPTANCE OF TRANSFER CREDIT AND ADVANCE STANDING
Applied Technology Academy reserves the right to determine eligible inbound credit for students seeking transfer credit. A student may apply for up to 75% of the total program hours in credit to an Applied Technology Academy program if approved by the President.

Credit for a course may be given for prior vendor certifications achieved that map to specific courses within a program. For example, if a student applies to attend the Preparation for Secure Infrastructure Specialist program, a program comprised of three 40 clock hours classes, CompTIA A+, CompTIA Network+ and CompTIA Security+, and the student has already achieved the CompTIA A+ certification from CompTIA, the school may grant 40 clock hours in credit for the CompTIA A+ course portion of the program.

Proof of prior vendor certification achievement for course credit must be provided by the student. Vendor certifications will be verified with the vendor and must be active and not expired. All vendor certifications are granted on a Pass/Fail basis and only passed, and active vendor certifications will be considered. Credit may also be given for relevant course work that

is documented by official transcript from another licensed post-secondary institution or accredited institution.

The transfer of credit from Applied Technology Academy to other institutions is solely within the purview of the accepting institution. Students who wish to transfer credit earned from Applied Technology Academy should consult with the admissions department of the Institution with which they choose to continue their education. Transferability of credit is at the discretion of the accepting institution, and it is the student's responsibility to confirm whether credits will be accepted by another institution of the student's choice.

REGISTRATION AND PAYMENT:
Students are required to submit a completed Student Enrollment Agreement no later than 5 business days prior to the start date of their program. Full program payment must be submitted to the school prior to the start date of the student's program.

ACADEMIC INFORMATION

GRADUATION REQUIREMENTS

A certificate is presented to the Student that has:

1. Successfully completed all required courses in the selected program.
2. Attended all required class hours.
3. Completed all required lab and course assignments.
4. Fulfilled all monetary obligations to the school.

GRADING SYSTEM

Our grading system is pass/fail as required by vendor certification. Students are graded during each course of study on a Pass/Fail basis by the instructor's evaluation of the product knowledge and the ability to follow instructions. General in class grading will be based on:

- Attendance: 50% of grade
- Lab and Course Assignments: 50% of grade

Student must be present in 80% of classes and must participate in 80% of course labs and assignments or else they will be put on academic probation. If the student falls below the 80% attendance and/or lab and assignment completion, the student will be evaluated on course content and asked to re-sit the course at a later date if needed. All students will be given one additional training period after they are put on probation to meet requirements or will be terminated at that time. Students are not terminated for failure to acquire skills but are encouraged to repeat classes or attend additional classes combined with furthered self-study.

Students receive program Certificates of Completion at the end of each program if the above requirements are met. All students have the option of refreshing classes for one year while it is being offered at no additional cost.

Students seeking additional vendor certification(s) will be tested for each student selected class within the program if they have successfully received their Certificate of Completion from Applied Technology Academy. These are proctored exams issued by a specific program vendor, which the student has chosen based upon their program of study. This testing has a different grade scale for each exam as dictated by the program vendors. Upon testing and passing the selected exams from within the program, the student will receive a Vendor Certification for that specific program directly from the vendor responsible for the certification and exam standards. If a student fails a vendor certification exam, they will be able to re-take the exam at their own cost.

RULES AND REGULATIONS

A. Attendance/Class Cuts:

An overall attendance of at least 80% is required to be considered passing. Instructors take attendance on a daily basis through an attendance log that is submitted to student services each day. On that attendance log, instructors mark whether the student present or absent. If

attendance falls under 80% the student will be considered failing and will have to set up a retake of their course through student services.

Any student that falls below 80% attendance while in a Program will be terminated from that program and the last date of attendance will be recorded. If a student wishes to re-enroll into the Program, the student will be re-enrolled and given prior credit for any of the classes that were previously attended.

B. Tardiness:
A student arriving after attendance has been taken is considered late. The instructor will mark the amount of time unless the instructor considers the reason for tardiness legitimate. All class time missed in excess of 15 minutes must be made up by the student prior to graduation. If the student arrives late and instructor cannot catch up student without interrupting the others in class, the student may be required to make up the entire day.

C. Conduct:
Students are always expected to conduct themselves in a professional and adult manner. Foul language, sexual harassment, possession of non-prescribed drugs, possession of alcoholic beverages, or disrespectful behavior is considered unsatisfactory conduct and may be grounds for dismissal. Theft of property from the school or other students is grounds for immediate dismissal. A student who conducts himself in a manner detrimental to the school, staff or other students will be terminated.

D. Make up work:
Students absent for any reason are required to make up any missed classes before proceeding to the next course of study. A student may make up missed time by attending another class in session or attending Saturday or night classes, which are conducted for other students.

E. Probation:
A student that does not adhere to the attendance policy will be placed on probation for 30 days. Should the student be absent while on probation, he will be counseled by the President/Director of Education, which could result in termination.

F. Interruptions in Training/Termination:
A student is not terminated for failure to learn the required skills. A student that has not successfully completed the lab and course assignments at the end of each course is encouraged to attend future additional class sessions for extra review and learning. The student is permitted to retake the classes within one year of their program start date. The retaking of such classes is of no extra cost to the student. If the student fails to achieve a passing grade the second time, he/she is counseled by the Student Navigator as to the advisability of continuing and that if he/she decides to continue a Certificate of Completion may not be awarded.

G. Leaves of Absence:
A student may be granted a leave of absence for a reasonable amount of time as determined by the Student Navigator (a 60-day maximum). A request for a leave of absence must be in writing and the date of expected return must be specified.

H. Re-entry:
A student that has canceled or has been terminated and desires to re-enter the program of study must notify the school and follow the required admission procedures. A student that was terminated for any reason must have an interview with the Student Navigator and show cause why he/she should be re-instated. The decision of the President/Director of Education is final.

APPEAL / COMPLAINT PROCEDURES
Any student who has a grievance with the school or an instructor should discuss the problem first with the instructor or may contact the Training Manager at 800-674-3550 during normal school hours. If a resolution is not reached, the student should make a written appeal and/or complaint and submit it to the school President, who is the appointed student complaint designee. If necessary, other students will be interviewed to determine the validity of the appeal and/or complaint. The student will receive a written response within 14 days following the receipt of the appeal and/or complaint, which shall include a summary of the institution's investigation and disposition of the appeal and/or complaint.

Applied Technology Academy is licensed by the Commission for Independent Education, Florida Department of Education. Additional information regarding this institution and/or complaint issues may be directed to the Commission at the address below.

Commission for Independent Education, Florida Department of Education
325 West Gaines Street, Suite 1414
Tallahassee, Florida 32399-0400
888-224-6684

CLOCK HOUR DEFINITION
Applied Technology Academy measures academic progress using the clock hour system. A Clock Hour means a period of 60 minutes with a minimum of 50 minutes of instruction in the presence of an instructor.

COURSE NUMBERING SYSTEM
Our course numbering system aligns with the CAPE Approved Course List Numbers. Courses that are not on the CAPE Approved List have a seven to eight digit alpha-numeric identifier. The prefix identifies the subject/vendor and the numeric portion identifies the vendor course reference.

CLASS STARTING & ENDING DATES
The school recommends that the student take the classes in the order listed under the program curriculum. All classes in a program will be scheduled sequentially in the Academic Calendar by

ATA. The date of completion is determined by the date that the student completes all of the required classes for each program. All classes are awarded a Certificate upon completion of the program. To obtain a program Certificate, all classes in the specific program must be completed.

A student may get counseling from their assigned Student Navigator and alter the speed of the program if the schedule permits. Students may repeat any class as many times as they wish up to one year from first day of each class start date. Students must retain their books and student resources from their original class that they want to repeat.

All Program start and end dates are identified by a Student Navigator on the Student Enrollment Agreement.

ACADEMIC CALENDAR

Applied Technology Academy does not operate on a traditional quarters or semesters calendar. Program scheduling is established every six months.

- The school is on a rolling calendar system.
- Programs/Classes are added throughout the year based on student demand.
- The school recommends that the student take the classes in the order listed under the program curriculum. The school schedules classes sequentially based on the order listed within the program curriculum.
- All Program start and end dates are identified by a Student Navigator on the Student Enrollment Agreement.

Academic Calendar - August, 2022 to August, 2023		
Program Name	**Clock Hours**	**Start Date***
Preparation for Secure Infrastructure Specialist	120	8/22/2022, 11/28/22, 1/16/23, 3/27/23, 6/19/23
Preparation for Computer Networking Professional	120	11/28/22, 1/16/23, 3/27/23, 6/19/23
Preparation for Computer Network Security Professional	120	1/30/23, 5/29/23, 7/10/23
Preparation for Networking Security and Cloud Technology Professional	200	12/12/2022, 03/20/2022
Preparation for Cybersecurity Professional	160	1/30/23, 5/29/23
Preparation for Advanced Cybersecurity Professional	80	1/16/2023, 5/15/2023
Preparation for Linux Network Professional	80	6/5/2023

Preparation for Python Programming Professional	80	3/6/2023, 7/10/23
Preparation for Cisco Certified Network Administrator	40	1/29/2023, 3/20/2023, 5/15/2023
Preparation for Cisco Certified Network Enterprise Professional	80	11/28/2023, 2/13/2023, 5/29/2023
Preparation for Microsoft Modern Desktop Administrator Associate	80	4/10/2023, 7/17/2023
Preparation for Microsoft 365 and Azure Security Administrator Associate	80	1/30/2023, 4/3/2023
Preparation for Microsoft Enterprise Administrator Expert	80	3/6/2023
Preparation for ITIL Foundations	36	12/12/2023, 2/6/2023
Preparation for Project Management and Six Sigma Professional	105	2/13/2023, 5/15/2023
Preparation for Certified Six Sigma Green Belt Professional	32.5	4/17/23
Preparation for Adobe Certified Associate	120	To be removed
*** Program dates may change due to low enrollment.**		

HOLIDAYS

Classes will not be held on the following holidays:

New Year's Day
Memorial Day
Independence Day
Labor Day
Thanksgiving Day
Christmas Day

CLASS CANCELLATION POLICY

Applied Technology Academy reserves the right to cancel a program due to low enrollment or circumstances beyond its control with a 14-day notice, prior to the proposed program start date for the student. Every effort will be made to reschedule a canceled class or transfer enrollment to a later date without undue hardship or penalty. If the school cancels a course or class etc., the student is entitled to a refund of all monies paid.

STUDENT SERVICES

STUDENT SERVICES
The Applied Technology Academy facility offers students a break room and a study area for their convenience.

A. Housing:
The school does not maintain housing for students. A list of reliable realtors and rental properties near the school will be provided to the student that requests housing assistance at the time of enrollment.

B. Student Records:
Student records are permanently retained by the school and are available to students upon individual request. Progress is readily available to students via their test results. Student records will be provided to potential employers only after the student has made written request.

C. Testing:
Certification testing is provided on site at the school for some vendor exams if attending in person for a Monday through Friday class, or an exam voucher is provided for the student to test at a public testing center or online testing resource at their convenience. All testing records are maintained by the school. The student is provided with copies of all testing results upon test completion.

D. Qualifications:
The test is monitored by a test Center Administrator/Proctor who has been certified by the exam platform vendor.

E. Student Placement:
Employment assistance is given by the school's Student Navigators to students. In addition, the instructors are available for test preparation review & counseling on skills development necessary in the technical job market. Instructors are also available as a technical reference after successful program completion.

Applied Technology Academy will notify any students of job availability and provide contact names and addresses of employment possibilities as they become available to the school. Applied Technology Academy will also refer students to our network of employment recruiters throughout the country. We will make introductions on behalf of our students, but the students must follow up with prospective employers and recruiters and continue career search communication independent of Applied Technology Academy.

There are currently no special requirements or physical limitations for employment in the industries for which Applied Technology Academy provides training. Applied Technology

Academy strongly recommends third party certification where appropriate, such as those offered by Microsoft, Cisco, EC-Council and CompTIA to enhance employment prospects.

No guarantee of placement is made or implied on behalf of Applied Technology Academy. We can provide statistically verified market and job availability; however, Applied Technology Academy does not promise or imply any specific market or job availability for our students.

F. Financial Aid: The school does not currently offer financial aid.

ENROLLMENT AGREEMENT

Prospective students may enroll anytime. Late enrollments will be only one week prior to class start time and as late as one day into first class, depending on the program and if the student has adequate experience.

Students will be notified of any changes made at the institution within a reasonable timeframe.

Students enrolling in a Certificate program will receive a Student Enrollment Agreement stating the registration fee, total tuition cost of the program and the included cost of books and supplies. Students re-entering the School in a Certificate program will also receive a Student Enrollment Agreement with tuition and fees based on the prevailing tuition and fee schedule at the time of re-entry.

CANCELLATION AND REFUND POLICY

Should a student's enrollment be terminated or cancelled for any reason, all refunds will be made according to the following refund schedule:

1. Cancellations can be made in person, by electronic mail, by Certified Mail or by termination.
2. All monies will be refunded if the school does not accept the applicant or if the student cancels within three (3) business days after signing the enrollment agreement and making initial payment.
3. Cancellation after the third (3rd) Business Day, but before the first class, will result in a refund of all monies paid, with the exception of the registration fee (not to exceed $150.00).
4. Cancellation after attendance has begun, through 40% completion of the program, will result in a Pro Rata refund computed on the number of hours completed to the total program hours and the cost of any courseware and course labs.
5. Cancellation after completing more than 40% of the program will result in no refund.
6. Termination Date: When calculating the refund due to a student, the last date of actual attendance by the student is used in the calculation unless earlier written notice was received.
7. A student can be terminated for insufficient progress, nonpayment of costs, or failure to comply with the rules.
8. Refunds will be made within 30 days of termination of the student's enrollment or receipt of a Cancellation Notice from the student.

GROUNDS FOR TERMINATION

Any student may be dismissed for violations of rules and regulations of the school, as set forth in the school's catalog. A student also may be withdrawn from classes if he or she does not prepare sufficiently, neglects assignments, or makes unsatisfactory progress. The President, after consultation with all parties involved, makes the final decision.

PROGRAMS OF STUDY AND LOCATION OFFERINGS

CERTIFICATE PROGRAMS - All programs are offered in a synchronous hybrid format. Students may take the courses in each program in person or via distance learning, or a combination of both.

COMPUTER PROGRAMS:

- Preparation for Secure Infrastructure Specialist
- Preparation for Computer Networking Professional
- Preparation for Computer Network Security Professional
- Preparation for Networking Security and Cloud Technology Professional
- Preparation for Cybersecurity Professional
- Preparation for Advanced Cybersecurity Professional
- Preparation for Linux Network Professional
- Preparation for Python Programming Professional
- Preparation for Cisco Certified Network Administrator
- Preparation for Cisco Certified Network Enterprise Professional
- Preparation for Microsoft Modern Desktop Administrator Associate
- Preparation for Microsoft 365 and Azure Security Administrator Associate
- Preparation for Microsoft Enterprise Administrator Expert
- Preparation for ITIL Foundations
- Preparation for Project Management and Six Sigma Professional
- Preparation for Certified Six Sigma Green Belt Professional
- Preparation for Adobe Certified Associate

DISTANCE LEARNING PROGRAMS:

- Preparation for Secure Infrastructure Specialist
- Preparation for Computer Networking Professional
- Preparation for Computer Network Security Professional
- Preparation for Networking Security and Cloud Technology Professional
- Preparation for Cybersecurity Professional
- Preparation for Advanced Cybersecurity Professional
- Preparation for Linux Network Professional
- Preparation for Python Programming Professional
- Preparation for Cisco Certified Network Administrator
- Preparation for Cisco Certified Network Enterprise Professional
- Preparation for Microsoft Modern Desktop Administrator Associate
- Preparation for Microsoft 365 and Azure Security Administrator Associate
- Preparation for Microsoft Enterprise Administrator Expert
- Preparation for ITIL Foundations
- Preparation for Project Management and Six Sigma Professional
- Preparation for Certified Six Sigma Green Belt Professional
- Preparation for Adobe Certified Associate

Preparation for Secure Infrastructure Specialist

Distance Learning (Online) and Fort Walton Beach

The Secure Infrastructure Specialist Program is designed to provide an individual with the computer knowledge and opportunity to prepare them for a career in IT, advance their current IT career and to prepare for three industry certifications. The certifications that are addressed in this preparatory program include A+, Net+ and Sec+. At the completion of this program you are qualified to manage, support, and troubleshoot information systems in a help desk environment. This course is based on lectures, discussions, demonstrations, exercises, and laboratory projects.

Program Objective:
The Secure Infrastructure Specialist program is designed to provide an individual with the computer knowledge that will prepare them for a career in the IT industry. The objective of the program is to help the student prepare to obtain the CompTIA A+, CompTIA Network+ and CompTIA Security+ certifications.

Program Requirements:
A secondary degree (High School Diploma, Associates degree or global equivalent.) Proficiency using the Windows environment and general knowledge of Hardware and Network concepts, but computer knowledge or experience is not required.

COURSE TITLE	CLOCK HOURS
COMPT001 – CompTIA A+	40
COMPT006 – CompTIA Network+	40
COMPT008 – CompTIA Security+	40
PROGRAM TOTAL	**120.0**

CompTIA A+ Prep

Subject Description

In this course, the student will install, configure, optimize, troubleshoot, repair, upgrade, and perform preventive maintenance on personal computers, digital devices, and operating systems.

Subject Hours
40 hours total:

- 20 hours lecture
- 20 hours lab

Course Objectives

- Upon Install and configure PC system unit components and peripheral devices.
- Install, configure, and troubleshoot display and multimedia devices.
- Install, configure, and troubleshoot storage devices.
- Install, configure, and troubleshoot internal system components.
- Explain network infrastructure concepts.
- Configure and troubleshoot network connections.
- Implement client virtualization and cloud computing.
- Support and troubleshoot laptops.
- Support and troubleshoot mobile devices.
- Install, configure, and troubleshoot print devices.

Instructional Methods

- Lecture
- Overhead slides
- Labs (virtual)
- Hand on in-class PC build
- Videos
- Assessments

Introductions/Policy Overview/Course Description

Lesson 1: Installing and Configuring PC Components

Topic A: Use Appropriate Safety Procedures
Topic B: PC Components
Topic C: Common Connection Interfaces
Topic D: Install Peripheral Devices
Topic E: Troubleshooting Methodology
Labs: 1.1.3; 1.1.5; 1.2.7; 2.5.6;

Lesson 2: Installing, Configuring, and Troubleshooting Display and Multimedia Devices

Topic A: Install and Configure Display Devices
Topic B: Troubleshoot Display Devices
Topic C: Install and Configure Multimedia Devices
Labs: 3.12.5; 3.13.7;

Lesson 3: Installing, Configuring, and Troubleshooting Storage Devices

Topic A: Install System Memory
Topic B: Install and Configure Mass Storage Devices
Topic C: Install and Configure Removable Storage
Topic D: Configure RAID
Topic E: Troubleshoot Storage Devices
Lab: 3.8.3; 3.8.7; 3.9.4; 3.9.5; 3.11.4;

Lesson 4: Installing, Configuring, and Troubleshooting Internal System Components

Topic A: Install and Upgrade CPUs
Topic B: Configure and Update BIOS/UEFI
Topic C: Install Power Supplies

Topic D: Troubleshoot Internal System Components
Topic E: Configure a Custom PC
Labs: Internal Components - 3.2.5; 3.3.5; 3.4.3; 3.4.4; 3.5.7; 3.6.3; 3.6.4;
Labs: Peripheral - 4.1.3; 4.2.3;

Lesson 5: Network Infrastructure Concepts
Topic A: Wired Networks
Topic B: Network Hardware Devices
Topic C: Wireless Networks
Topic D: Internet Connection Types
Topic E: Network Configuration Concepts
Topic F: Network Services
Labs: Wired - 6.2.6; 6.6.5; 6.6.6; 6.8.3; 6.8.4; (build a CAT 5 cable and test)
Labs: Wireless - 7.1.7; 7.1.8; 7.1.9; 7.1.10; 7.3.7; 7.4.4; 7.5.3 (practice questions)

Lesson 6: Configuring and Troubleshooting Networks
Topic A: Configure Network Connection Settings
Topic B: Install and Configure SOHO Networks
Topic C: Configure SOHO Network Security
Topic D: Configure Remote Access
Topic E: Troubleshoot Network Connections
Topic F: Install and Configure IoT Devices
Labs: 6.9.3; 6.9.4; 6.9.5; 6.9.6; 6.10.4; 6.10.5

Lesson 7: Implementing Client Virtualization and Cloud Computing
Topic A: Configure Client-Side Virtualization
Topic B: Cloud Computing Concepts
Labs: No labs

Lesson 8: Supporting and Troubleshooting Laptops
Topic A: Use Laptop Features
Topic B: Install and Configure Laptop Hardware
Topic C: Troubleshoot Common Laptop Issues
Labs: 9.3.5; 9.3.6; 9.4.5 (practice questions)

Lesson 9: Supporting and Troubleshooting Mobile Devices
Topic A: Mobile Device Types
Topic B: Connect and Configure Mobile Device Accessories
Topic C: Configure Mobile Device Network Connectivity
Topic D: Support Mobile Apps
Topic E: Secure Mobile Devices
Topic F: Troubleshoot Mobile Device Issues
Labs: 9.6.7; 9.7.4;

Lesson 10: Installing, Configuring, and Troubleshooting Print Devices
Topic A: Maintain Laser Printers
Topic B: Maintain Inkjet Printers
Topic C: Maintain Impact, Thermal, and 3D Printers

Topic D: Install and Configure Printers
Topic E: Troubleshoot Print Device Issues
Topic F: Install and Configure Imaging Devices
Labs: 4.3.3; 4.5.8; 4.6.4; 4.6.5

Non-Virtual Labs:

Operational Procedures - create and deploy an image using Clonezilla; configure Windows backup; install an OS; connect it to the network; connect it to a printer - using all our devices
14.4 - Create a home office network; install and configure a wireless router (using one we provide)
14.6 - Troubleshoot a mobile device
Students need a USB drive for Clonezilla; CD to put the OS on; external hard drives to store/deploy the image.

Evaluation Time: After the last lesson of class, students will be given 20 minutes to log and complete the evaluation for their class.

Assessment: 1 hour timed assessment (Break for 30 or 60-minute lunch)

Assessment Review: If the assessment score is lower than 70%, after the initial assessment review the student will have option to retake another assessment.

CompTIA Network+ Prep

Course Overview

This course is designed to provide network technicians and support staff with the foundation-level skills they need to install, operate, manage, maintain, and troubleshoot a corporate network.

Course Objectives

Upon completion of this course, students will be able to:

- Identify the basic components of network theory.
- Identify the major network communications methods.
- Identify network data delivery methods.
- List and describe network media and hardware components.
- Identify the major types of network implementations.
- Identify the components of a TCP/IP network implementation.
- List the major services deployed on TCP/IP networks.
- Identify characteristics of a variety of network protocols.
- Identify the components of a LAN implementation.
- Identify the components of a WAN implementation.
- Identify major issues and technologies in network security.
- Identify the components of a remote network implementation.
- Identify major issues and technologies in disaster recovery.
- Identify major data storage technologies and implementations.
- Identify the primary network operating systems.

- Identify major issues, models, tools, and techniques in network troubleshooting.

Instructional Methods

- Lecture
- Overhead slides
- Lab

Course Outline

Chapter 1: Fundamentals
- Module A: Networking concepts
- Module B: Classifying networks
- Module C: Network models
- Module D: The troubleshooting process

Chapter 2: Physical networks
- Module A: Connection technologies
- Module B: Network devices
- Module C: Copper media
- Module D: Optical media
- Module E: Ethernet standards

Chapter 3: TCP/IP networks
- Module A: IP addressing
- Module B: Core protocols
- Module C: Network ports and applications

Chapter 4: Internetworking
- Module A: Switching
- Module B: Routing

Chapter 5: Wireless LANs
- Module A: Wireless networks
- Module B: Wireless LAN standards

Chapter 6: Wide area networks
- Module A: Internet connections
- Module B: WAN infrastructure

Chapter 7: Cybersecurity principles
- Module A: Goals and threats
- Module B: Digital security
- Module C: Transport encryption

Chapter 8: Defending networks
- Module A: Network security components
- Module B: Network authentication systems

- Module C: Hardening networks

Chapter 9: Evolving network technologies
- Module A: Network convergence
- Module B: Virtual and cloud systems

Chapter 10: Network operations
- Module A: Monitoring and optimization
- Module B: Fault tolerance and disaster recovery
- Module C: Incident response

Chapter 11: Network planning
- Module A: Network policy design
- Module B: Network installation
- Module C: Maintenance and upgrades

CompTIA Security+ Prep

Course Overview

This course will prepare students to pass the current CompTIA Security+ SY0-501 certification. After taking this course, students will understand the field of network security and how it relates to other areas of information technology. This course also provides the broad-based knowledge necessary to prepare for further study in specialized security fields, or it can serve as a capstone course that gives a general introduction to the field.

Course Objectives

Upon completion of this course, students will be able to:

- Identify security threats.
- Harden internal systems and services.
- Harden internetwork devices and services.
- Secure network communications.
- Manage a PKI.
- Manage certificates.
- Enforce an organizational security policy.
- Monitor the security infrastructure.

Instructional Methods

- Lecture
- Overhead slides
- Lab exercises

Course Outline

Chapter 1: Security Fundamentals
- Module A: Security concepts
- Module B: Risk management

- Module C: Vulnerability assessment

Chapter 2: Understanding attacks
- Module A: Understanding attackers
- Module B: Social engineering
- Module C: Malware
- Module D: Network attacks
- Module E: Application attacks

Chapter 3: Cryptography
- Module A: Cryptography concepts
- Module B: Public key infrastructure

Chapter 4: Network fundamentals
- Module A: Network components
- Module B: Network addressing
- Module C: Network ports and applications

Chapter 5: Securing networks
- Module A: Network security components
- Module B: Transport encryption
- Module C: Hardening networks
- Module D: Monitoring and detection

Chapter 6: Securing hosts and data
- Module A: Securing hosts
- Module B: Securing data
- Module C: Mobile device security

Chapter 7: Securing network services
- Module A: Securing applications
- Module B: Virtual and cloud systems

Chapter 8: Authentication
- Module A: Authentication factors
- Module B: Authentication protocols

Chapter 9: Access control
- Module A: Access control principles
- Module B: Account management

Chapter 10: Organizational security
- Module A: Security policies
- Module B: User training
- Module C: Physical security and safety

Chapter 11: Disaster planning and recovery
- Module A: Business continuity

- Module B: Fault tolerance and recovery
- Module C: Incident response

Preparation for Computer Networking Professional

Distance Learning (Online) and Fort Walton Beach

At the completion of this program you are qualified to manage, support, and troubleshoot information systems in a wide range of computing environments with Microsoft Windows Server and the integrated family of server products. Additionally, the course will provide the concepts, commands, and practice required to configure Cisco switches and routers in multi-protocol Internet works. This course is based on lectures, discussions, demonstrations, exercises, and laboratory projects. Students perform all basic configuration procedures to build LAN and WAN interfaces for the most used routing and routed protocols. In addition, the student will be taught the knowledge to prepare for both the Network+ and the Security+ certifications and the skills to understand the core components of establishing networks and securing IT assets.

Program Objective:
To prepare obtain the CompTIA Network+, CompTIA Security+ and the Cisco CCNA certifications.

Program Requirements:
A secondary degree (High School Diploma, Associates degree or global equivalent.) Proficiency using the Windows environment and general knowledge of Hardware and Network concepts, but computer knowledge or experience is not required.

COURSE TITLE	CLOCK HOURS
COMPT006 – CompTIA Network+ Certification	40
COMPT008 – CompTIA Security+ Certification	40
CISCO301 – Implementing and Administering Cisco Solutions	40
PROGRAM TOTAL	**120.0**

CompTIA Network+ Prep

Course Overview
This course is designed to provide network technicians and support staff with the foundation-level skills they need to install, operate, manage, maintain, and troubleshoot a corporate network.

Course Objectives
Upon completion of this course, students will be able to:

- Identify the basic components of network theory.
- Identify the major network communications methods.
- Identify network data delivery methods.
- List and describe network media and hardware components.
- Identify the major types of network implementations.
- Identify the components of a TCP/IP network implementation.
- List the major services deployed on TCP/IP networks.

- Identify characteristics of a variety of network protocols.
- Identify the components of a LAN implementation.
- Identify the components of a WAN implementation.
- Identify major issues and technologies in network security.
- Identify the components of a remote network implementation.
- Identify major issues and technologies in disaster recovery.
- Identify major data storage technologies and implementations.
- Identify the primary network operating systems.
- Identify major issues, models, tools, and techniques in network troubleshooting.

Instructional Methods

- Lecture
- Overhead slides
- Lab

Course Outline

Chapter 1: Fundamentals
- Module A: Networking concepts
- Module B: Classifying networks
- Module C: Network models
- Module D: The troubleshooting process

Chapter 2: Physical networks
- Module A: Connection technologies
- Module B: Network devices
- Module C: Copper media
- Module D: Optical media
- Module E: Ethernet standards

Chapter 3: TCP/IP networks
- Module A: IP addressing
- Module B: Core protocols
- Module C: Network ports and applications

Chapter 4: Internetworking
- Module A: Switching
- Module B: Routing

Chapter 5: Wireless LANs
- Module A: Wireless networks
- Module B: Wireless LAN standards

Chapter 6: Wide area networks
- Module A: Internet connections
- Module B: WAN infrastructure

Chapter 7: Cybersecurity principles

- Module A: Goals and threats
- Module B: Digital security
- Module C: Transport encryption

Chapter 8: Defending networks
- Module A: Network security components
- Module B: Network authentication systems
- Module C: Hardening networks

Chapter 9: Evolving network technologies
- Module A: Network convergence
- Module B: Virtual and cloud systems

Chapter 10: Network operations
- Module A: Monitoring and optimization
- Module B: Fault tolerance and disaster recovery
- Module C: Incident response

Chapter 11: Network planning
- Module A: Network policy design
- Module B: Network installation
- Module C: Maintenance and upgrades

CompTIA Security+ Prep

Course Overview

This course will prepare students to pass the current CompTIA Security+ SY0-501 certification. After taking this course, students will understand the field of network security and how it relates to other areas of information technology. This course also provides the broad-based knowledge necessary to prepare for further study in specialized security fields, or it can serve as a capstone course that gives a general introduction to the field.

Course Objectives

Upon completion of this course, students will be able to:

- Identify security threats.
- Harden internal systems and services.
- Harden internetwork devices and services.
- Secure network communications.
- Manage a PKI.
- Manage certificates.
- Enforce an organizational security policy.
- Monitor the security infrastructure.

Instructional Methods

- Lecture

- Overhead slides
- Lab exercises

Course Outline

Chapter 1: Security Fundamentals

- Module A: Security concepts
- Module B: Risk management
- Module C: Vulnerability assessment

Chapter 2: Understanding attacks

- Module A: Understanding attackers
- Module B: Social engineering
- Module C: Malware
- Module D: Network attacks
- Module E: Application attacks

Chapter 3: Cryptography

- Module A: Cryptography concepts
- Module B: Public key infrastructure

Chapter 4: Network fundamentals

- Module A: Network components
- Module B: Network addressing
- Module C: Network ports and applications

Chapter 5: Securing networks

- Module A: Network security components
- Module B: Transport encryption
- Module C: Hardening networks
- Module D: Monitoring and detection

Chapter 6: Securing hosts and data

- Module A: Securing hosts
- Module B: Securing data
- Module C: Mobile device security

Chapter 7: Securing network services

- Module A: Securing applications
- Module B: Virtual and cloud systems

Chapter 8: Authentication

- Module A: Authentication factors
- Module B: Authentication protocols

Chapter 9: Access control

- Module A: Access control principles
- Module B: Account management

Chapter 10: Organizational security

- Module A: Security policies
- Module B: User training
- Module C: Physical security and safety

Chapter 11: Disaster planning and recovery

- Module A: Business continuity
- Module B: Fault tolerance and recovery
- Module C: Incident response

Cisco CCNA v1.0 – Implementing and Administering Cisco

Course Overview

The Implementing and Administering Cisco Solutions (CCNA) v1.0 course gives you a broad range of fundamental knowledge for all IT careers. Through a combination of lecture and hands-on labs, you will learn how to install, operate, configure, and verify basic IPv4 and IPv6 networks. The course covers configuring network components such as switches, routers, and wireless LAN controllers; managing network devices; and identifying basic security threats. The course also gives you a foundation in network programmability, automation, and software-defined networking.

This course helps you prepare to take the 200-301 Cisco® Certified Network Associate (CCNA®) exam. By passing this one exam, you earn CCNA certification.

Course Objectives

- Identify the components of a computer network and describe their basic characteristics
- Understand the model of host-to-host communication
- Describe the features and functions of the Cisco Internetwork Operating System (IOS®) software
- Describe LANs and the role of switches within LANs
- Describe Ethernet as the network access layer of TCP/IP and describe the operation of switches
- Install a switch and perform the initial configuration
- Describe the TCP/IP Internet layer, IPv4, its addressing scheme, and subnetting
- Describe the TCP/IP Transport layer and Application layer
- Explore functions of routing
- Implement basic configuration on a Cisco router
- Explain host-to-host communications across switches and routers
- Identify and resolve common switched network issues and common problems associated with IPv4 addressing
- Describe IPv6 main features and addresses, and configure and verify basic IPv6 connectivity
- Describe the operation, benefits, and limitations of static routing
- Describe, implement, and verify virtual local area networks (VLANs) and trunks
- Describe the application and configuration of inter-VLAN routing

- Explain the basics of dynamic routing protocols and describe components and terms of Open Shortest Path First (OSPF)
- Explain how Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) work
- Configure link aggregation using EtherChannel
- Describe the purpose of Layer 3 redundancy protocols
- Describe basic WAN and VPN concepts
- Describe the operation of access control lists (ACLs) and their applications in the network
- Configure Internet access using Dynamic Host Configuration Protocol (DHCP) clients and explain and configure network address translation (NAT) on Cisco routers
- Describe basic quality of service (QoS) concepts
- Describe the concepts of wireless networks, which types of wireless networks can be built, and how to use Wireless LAN Controllers (WLCs)
- Describe network and device architectures and introduce virtualization
- Introduce the concept of network programmability and Software-Defined Networking (SDN) and describe smart network management solutions such as Cisco DNA Center™, Software-Defined Access (SD-Access), and Software-Defined Wide Area Network (SD-WAN)
- Configure basic IOS system monitoring tools
- Describe the management of Cisco devices
- Describe the current security threat landscape
- Describe threat defense technologies
- Implement a basic security configuration of the device management plane
- Implement basic steps to harden network devices

Course Outline

This class includes lecture sections and some self-study sections. In instructor-led classes, lectures are delivered in real-time, either in person or remote. The self-study sections are available online.

- Exploring the Functions of Networking
- Introducing the Host-to-Host Communications Model
- Operating Cisco IOS Software
- Introducing LANs
- Exploring the TCP/IP Link Layer
- Starting a Switch
- Introducing the TCP/IP Internet Layer, IPv4 Addressing, and Subnets
- Explaining the TCP/IP Transport Layer and Application Layer
- Exploring the Functions of Routing
- Configuring a Cisco Router
- Exploring the Packet Delivery Process
- Troubleshooting a Simple Network
- Introducing Basic IPv6
- Configuring Static Routing
- Implementing VLANs and Trunks

- Routing Between VLANs
- Introducing OSPF
- Building Redundant Switched Topologies (Self-study)
- Improving Redundant Switched Topologies with EtherChannel
- Exploring Layer 3 Redundancy (Self-study)
- Introducing WAN Technologies (Self-study)
- Explaining Basics of ACL
- Enabling Internet Connectivity
- Introducing QoS (Self-study)
- Explaining Wireless Fundamentals (Self-study)
- Introducing Architectures and Virtualization (Self-study)
- Explaining the Evolution of Intelligent Networks
- Introducing System Monitoring
- Managing Cisco Devices
- Examining the Security Threat Landscape (Self-study)
- Implementing Threat Defense Technologies (Self-study)
- Securing Administrative Access
- Implementing Device Hardening

Lab Outline

- Get Started with Cisco Command-Line Interface (CLI)
- Observe How a Switch Operates
- Perform Basic Switch Configuration
- Implement the Initial Switch Configuration
- Inspect TCP/IP Applications
- Configure an Interface on a Cisco Router
- Configure and Verify Layer 2 Discovery Protocols
- Implement an Initial Router Configuration
- Configure Default Gateway
- Explore Packet Forwarding
- Troubleshoot Switch Media and Port Issues
- Troubleshoot Port Duplex Issues
- Configure Basic IPv6 Connectivity
- Configure and Verify IPv4 Static Routes
- Configure IPv6 Static Routes
- Implement IPv4 Static Routing
- Implement IPv6 Static Routing
- Configure VLAN and Trunk
- Troubleshoot VLANs and Trunk
- Configure a Router on a Stick
- Implement Multiple VLANs and Basic Routing Between the VLANs

- Configure and Verify Single-Area OSPF
- Configure and Verify EtherChannel
- Improve Redundant Switched Topologies with EtherChannel
- Configure and Verify IPv4 ACLs
- Implement Numbered and Named IPv4 ACLs
- Configure a Provider-Assigned IPv4 Address
- Configure Static NAT
- Configure Dynamic NAT and Port Address Translation (PAT)
- Implement PAT
- Log into the WLC
- Monitor the WLC
- Configure a Dynamic (VLAN) Interface
- Configure a DHCP Scope
- Configure a WLAN
- Define a Remote Access Dial-In User Service (RADIUS) Server
- Explore Management Options
- Explore the Cisco DNA™ Center
- Configure and Verify NTP
- Configure System Message Logging
- Create the Cisco IOS Image Backup
- Upgrade Cisco IOS Image
- Configure WLAN Using Wi-Fi Protected Access 2 (WPA2) Pre-shared Key (PSK) Using the GUI
- Secure Console and Remote Access
- Enable and Limit Remote Access Connectivity
- Secure Device Administrative Access
- Configure and Verify Port Security
- Implement Device Hardening

Preparation for Computer Network Security Professional

Distance Learning (Online) and Fort Walton Beach

Cybersecurity Professionals are the protectors of our networks. They perform many duties which include analysis of data to identify vulnerabilities, threats, and risks to an organization. This includes configuration and tuning of threat-detection tools, and recurring applications and systems within an organization.

Both CND and Security+ are courses that validate the baseline skills necessary to perform core security functions and pursue an IT security career. PenTest+ is a certification that equips students for hands-on penetration testing to identify, exploit, report, and manage vulnerabilities on a network. Finally, CySA+ is an IT workforce certification that applies behavioral analytics to networks and devices to prevent, detect and combat cybersecurity threats.

Program Objective:
To prepare to obtain the EC-Council CND **OR** CompTIA Security+, CompTIA PenTest+, CompTIA CySA certifications.

Program Requirements:
A secondary degree (High School Diploma, Associates degree or global equivalent.) Proficiency using the Windows environment and general knowledge of Hardware and Network concepts, but computer knowledge or experience is not required.

COURSE TITLE	**CLOCK HOURS**
ICOEC001 – EC-Council Certified Network Defender	40
OR	
COMPT008 – CompTIA Security+ Certification	
COMPT017 - CompTIA PenTest+ Certification	40
COMPT016 - CompTIA CySA+ Certification	40
PROGRAM TOTAL	**120.0**

EC-Council Certified Network Defender

Course Overview
The EC-Council Certified Network Defender Course teaches real life situations involving basic network defense in a hands-on lab training format. This program is a professional level introduction to the cyber defense strategies needed in today's critical infrastructure. This course provides a comprehensive review of network defense fundamentals, the application of network security controls, protocols, perimeter appliances, secure IDS, VPN, and firewall configuration, and comprehensive exam preparation best practices.

Acquired Skills

- Install, configure, and manage network security controls and devices
- Design, implement, and monitor security policies
- Harden hosts to secure them against intrusions
- Implement and configure VNPs and wireless network technologies
- Perform risk, threat, and vulnerability assessments

Course Detail

1. Computer Network Defense Fundamentals
2. Network Security Threats, Vulnerabilities, and Attacks
3. Network Security Controls, Protocols, and Perimeter Appliances
4. Secure Firewall Configuration, Deployment and Management
5. Secure IDS Configuration and Management
6. Secure VPN Configuration and Management
7. Designing a Secure Network
8. Network Traffic Signatures and Analysis
9. Monitoring and Securing Network Traffic
10. Network Vulnerability Scanning
11. Monitoring and Securing Network Traffic
12. Network Vulnerability Scanning
13. Host/System Security
14. Physical Security
15. Designing and Implementation of Network Security Policies
16. Network Incident Response and Management
17. Network Backup and Disaster Recovery
18. Wireless Network Defense

Additional Information

Being well-versed in cyber security fundamentals is recommended. Basic network and host operations knowledge and experience commensurate with one to five years of network, host, or application administration.

OR

CompTIA Security+ Prep

Course Overview

This course will prepare students to pass the current CompTIA Security+ SY0-501 certification. After taking this course, students will understand the field of network security and how it relates to other areas of information technology. This course also provides the broad-based knowledge necessary to prepare for further study in specialized security fields, or it can serve as a capstone course that gives a general introduction to the field.

Course Objectives

Upon completion of this course, students will be able to:

- Identify security threats.
- Harden internal systems and services.
- Harden internetwork devices and services.
- Secure network communications.
- Manage a PKI.
- Manage certificates.
- Enforce an organizational security policy.
- Monitor the security infrastructure.

Instructional Methods

- Lecture
- Overhead slides
- Lab exercises

Course Outline

Chapter 1: Security Fundamentals

- Module A: Security concepts
- Module B: Risk management
- Module C: Vulnerability assessment

Chapter 2: Understanding attacks

- Module A: Understanding attackers
- Module B: Social engineering
- Module C: Malware
- Module D: Network attacks
- Module E: Application attacks

Chapter 3: Cryptography

- Module A: Cryptography concepts
- Module B: Public key infrastructure

Chapter 4: Network fundamentals

- Module A: Network components
- Module B: Network addressing
- Module C: Network ports and applications

Chapter 5: Securing networks

- Module A: Network security components
- Module B: Transport encryption
- Module C: Hardening networks
- Module D: Monitoring and detection

Chapter 6: Securing hosts and data

- Module A: Securing hosts
- Module B: Securing data
- Module C: Mobile device security

Chapter 7: Securing network services
- Module A: Securing applications
- Module B: Virtual and cloud systems

Chapter 8: Authentication
- Module A: Authentication factors
- Module B: Authentication protocols

Chapter 9: Access control
- Module A: Access control principles
- Module B: Account management

Chapter 10: Organizational security
- Module A: Security policies
- Module B: User training
- Module C: Physical security and safety

Chapter 11: Disaster planning and recovery
- Module A: Business continuity
- Module B: Fault tolerance and recovery
- Module C: Incident response

Grading
Grading will be assigned as follows:

- Attendance: 50%
- Lab Assignments: 50%

CompTIA Pentest+ Prep

Course Overview
As organizations scramble to protect themselves and their customers against privacy or security breaches, the ability to conduct penetration testing is an emerging skill set that is becoming ever more valuable to the organizations seeking protection, and ever more lucrative for those who possess these skills. In this course, you will be introduced to general concepts and methodologies related to pen testing, and you will work your way through a simulated pen test for a fictitious company.

This course will assist you if you are pursuing the CompTIA PenTest+ certification, as tested in exam PT0-001.

Job Roles
• Penetration Tester
• Vulnerability Tester
• Security Analyst (II)

- Vulnerability Assessment Analyst
- Network Security Operations
- Application Security Vulnerability

Course Objectives

Lesson 1: Planning and Scoping Penetration Tests

Topic A: Introduction to Penetration Testing Concepts
Topic B: Plan a Pen Test Engagement
Topic C: Scope and Negotiate a Pen Test Engagement
Topic D: Prepare for a Pen Test Engagement

Lesson 2: Conducting Passive Reconnaissance

Topic A: Gather Background Information
Topic B: Prepare Background Findings for Next Steps

Lesson 3: Performing Non-Technical Tests

Topic A: Perform Social Engineering Tests
Topic B: Perform Physical Security Tests on Facilities

Lesson 4: Conducting Active Reconnaissance

Topic A: Scan Networks
Topic B: Enumerate Targets
Topic C: Scan for Vulnerabilities
Topic D: Analyze Basic Scripts

Lesson 5: Analyzing Vulnerabilities

Topic A: Analyze Vulnerability Scan Results
Topic B: Leverage Information to Prepare for Exploitation

Lesson 6: Penetrating Networks

Topic A: Exploit Network-Based Vulnerabilities
Topic B: Exploit Wireless and RF-Based Vulnerabilities
Topic C: Exploit Specialized Systems

Lesson 7: Exploiting Host-Based Vulnerabilities

Topic A: Exploit Windows-Based Vulnerabilities
Topic B: Exploit *Nix-Based Vulnerabilities

Lesson 8: Testing Applications

Topic A: Exploit Web Application Vulnerabilities
Topic B: Test Source Code and Compiled Apps

Lesson 9: Completing Post-Exploit Tasks
Topic A: Use Lateral Movement Techniques
Topic B: Use Persistence Techniques
Topic C: Use Anti-Forensics Techniques

Lesson 10: Analyzing and Reporting Pen Test Results
Topic A: Analyze Pen Test Data
Topic B: Develop Recommendations for Mitigation Strategies
Topic C: Write and Handle Reports
Topic D: Conduct Post-Report-Delivery Activities

Appendix A: Mapping Course Content to CompTIA PenTest+

CySA+ - CompTIA Cybersecurity Analyst+

Course Overview
Students will learn about the duties of cybersecurity analysts who are responsible for monitoring and detecting security incidents in information systems and networks and for executing a proper response to such incidents. Students will gain the tools and tactics to manage cybersecurity risks, identify various types of common threats, evaluate an organization's security, collect and analyze cybersecurity intelligence, and handle incidents as they occur. This is a comprehensive approach to security aimed toward those on the front lines of defense.
In addition, this course can help students who are looking to fulfill DoD directive 8570.01 for information assurance (IA) training. This program is designed for personnel performing IA functions, establishing IA policies, and implementing security measures and procedures for the Department of Defense and affiliated information systems and networks. (CompTIA Cybersecurity Analyst Plus)

Acquired Skills
- Assess information security risk in computing and network environments.
- Analyze reconnaissance threats to computing and network environments.
- Analyze attacks on computing and network environments.
- Analyze post-attack techniques on computing and network environments.
- Implement a vulnerability management program.
- Collect cybersecurity intelligence.
- Analyze data collected from security and event logs.
- Perform active analysis on assets and networks.
- Respond to cybersecurity incidents.
- Investigate cybersecurity incidents.
- Address security issues with the organization's technology architecture.

Course Outline

Lesson 1: Assessing Information Security Risk
Topic A: Identify the Importance of Risk Management
Topic B: Assess Risk
Topic C: Mitigate Risk
Topic D: Integrate Documentation into Risk Management

Lesson 2: Analyzing Reconnaissance Threats to Computing and Network Environments
Topic A: Assess the Impact of Reconnaissance Incidents
Topic B: Assess the Impact of Social Engineering

Lesson 3: Analyzing Attacks on Computing and Network Environments
Topic A: Assess the Impact of System Hacking Attacks
Topic B: Assess the Impact of Web-Based Attacks
Topic C: Assess the Impact of Malware
Topic D: Assess the Impact of Hijacking and Impersonation Attacks
Topic E: Assess the Impact of DoS Incidents
Topic F: Assess the Impact of Threats to Mobile Security
Topic G: Assess the Impact of Threats to Cloud Security

Lesson 4: Analyzing Post-Attack Techniques
Topic A: Assess Command and Control Techniques
Topic B: Assess Persistence Techniques
Topic C: Assess Lateral Movement and Pivoting Techniques
Topic D: Assess Data Exfiltration Techniques
Topic E: Assess Anti-Forensics Techniques

Lesson 5: Managing Vulnerabilities in the Organization
Topic A: Implement a Vulnerability Management Plan
Topic B: Assess Common Vulnerabilities
Topic C: Conduct Vulnerability Scans
Topic D: Conduct Penetration Tests on Network Assets

Lesson 6: Collecting Cybersecurity Intelligence
Topic A: Deploy a Security Intelligence Collection and Analysis Platform
Topic B: Collect Data from Network-Based Intelligence Sources
Topic C: Collect Data from Host-Based Intelligence Sources

Lesson 7: Analyzing Log Data
Topic A: Use Common Tools to Analyze Logs
Topic B: Use SIEM Tools for Analysis

Lesson 8: Performing Active Asset and Network Analysis
Topic A: Analyze Incidents with Windows-Based Tools
Topic B: Analyze Incidents with Linux-Based Tools

Topic C: Analyze Malware
Topic D: Analyze Indicators of Compromise

Lesson 9: Responding to Cybersecurity Incidents
Topic A: Deploy an Incident Handling and Response Architecture
Topic B: Mitigate Incidents
Topic C: Prepare for Forensic Investigation as a CSIRT
Lesson 10: Investigating Cybersecurity Incidents
Topic A: Apply a Forensic Investigation Plan
Topic B: Securely Collect and Analyze Electronic Evidence
Topic C: Follow Up on the Results of an Investigation

Lesson 11: Addressing Security Architecture Issues
Topic A: Remediate Identity and Access Management Issues
Topic B: Implement Security During the SDLC
Appendix A: Mapping Course Content to CompTIA® Cybersecurity Analyst+ (Exam CS0-001)
Appendix B: Security Resources

Preparation for Networking Security and Cloud Technology Professional

Distance Learning (Online) and Fort Walton Beach

This program equips a student to learn how to design and implement a secure network infrastructure on a cloud platform. Through an understanding of security best practices and industry security requirements, the individual designs, develops, and manages a secure infrastructure leveraging varying technologies. Concepts taught will include managing identity and access management, defining organizational structure and policies, data protection, configuring network security defenses, collecting and analyzing logs, managing incident responses, and an understanding of regulatory concerns. In addition, advanced technical skills and knowledge around the design, management and securing of data, applications and infrastructure in the cloud using best practices, policies and procedures will also be taught.

Program Objective:
To obtain the CompTIA Network+, CompTIA Security+, CompTIA Cloud+, ISC^2 Certified Cloud Security Professional and the Cisco CCNA certifications.

Program Requirements:
A secondary degree (High School Diploma, Associates degree or global equivalent.) Proficiency using the Windows environment and general knowledge of Hardware and Network concepts, but computer knowledge or experience is not required.

COURSE TITLE	CLOCK HOURS
COMPT006 – CompTIA Network+ Certification	40
COMPT008 – CompTIA Security+ Certification	40
COMPT011 – CompTIA Cloud+ Certification	40
CISCO301 – CCNA Implementing and Administering Cisco Solutions	40
CCSP001 - ISC^2 Certified Cloud Security Professional	40
PROGRAM TOTAL	**200.0**

CompTIA Network+ Prep

Course Overview
This course is designed to provide network technicians and support staff with the foundation-level skills they need to install, operate, manage, maintain, and troubleshoot a corporate network.

Course Objectives
Upon completion of this course, students will be able to:

- Identify the basic components of network theory.
- Identify the major network communications methods.
- Identify network data delivery methods.
- List and describe network media and hardware components.
- Identify the major types of network implementations.

- Identify the components of a TCP/IP network implementation.
- List the major services deployed on TCP/IP networks.
- Identify characteristics of a variety of network protocols.
- Identify the components of a LAN implementation.
- Identify the components of a WAN implementation.
- Identify major issues and technologies in network security.
- Identify the components of a remote network implementation.
- Identify major issues and technologies in disaster recovery.
- Identify major data storage technologies and implementations.
- Identify the primary network operating systems.
- Identify major issues, models, tools, and techniques in network troubleshooting.

Instructional Methods

- Lecture
- Overhead slides
- Lab

Course Outline

Chapter 1: Fundamentals
- Module A: Networking concepts
- Module B: Classifying networks
- Module C: Network models
- Module D: The troubleshooting process

Chapter 2: Physical networks
- Module A: Connection technologies
- Module B: Network devices
- Module C: Copper media
- Module D: Optical media
- Module E: Ethernet standards

Chapter 3: TCP/IP networks
- Module A: IP addressing
- Module B: Core protocols
- Module C: Network ports and applications

Chapter 4: Internetworking
- Module A: Switching
- Module B: Routing

Chapter 5: Wireless LANs
- Module A: Wireless networks
- Module B: Wireless LAN standards

Chapter 6: Wide area networks

- Module A: Internet connections
- Module B: WAN infrastructure

Chapter 7: Cybersecurity principles
- Module A: Goals and threats
- Module B: Digital security
- Module C: Transport encryption

Chapter 8: Defending networks
- Module A: Network security components
- Module B: Network authentication systems
- Module C: Hardening networks

Chapter 9: Evolving network technologies
- Module A: Network convergence
- Module B: Virtual and cloud systems

Chapter 10: Network operations
- Module A: Monitoring and optimization
- Module B: Fault tolerance and disaster recovery
- Module C: Incident response

Chapter 11: Network planning
- Module A: Network policy design
- Module B: Network installation
- Module C: Maintenance and upgrades

CompTIA Security+ Prep

Course Overview

This course will prepare students to pass the current CompTIA Security+ SY0-501 certification. After taking this course, students will understand the field of network security and how it relates to other areas of information technology. This course also provides the broad-based knowledge necessary to prepare for further study in specialized security fields, or it can serve as a capstone course that gives a general introduction to the field.

Course Objectives

Upon completion of this course, students will be able to:

- Identify security threats.
- Harden internal systems and services.
- Harden internetwork devices and services.
- Secure network communications.
- Manage a PKI.
- Manage certificates.
- Enforce an organizational security policy.
- Monitor the security infrastructure.

Instructional Methods

- Lecture
- Overhead slides
- Lab exercises

Course Outline

Chapter 1: Security Fundamentals

- Module A: Security concepts
- Module B: Risk management
- Module C: Vulnerability assessment

Chapter 2: Understanding attacks

- Module A: Understanding attackers
- Module B: Social engineering
- Module C: Malware
- Module D: Network attacks
- Module E: Application attacks

Chapter 3: Cryptography

- Module A: Cryptography concepts
- Module B: Public key infrastructure

Chapter 4: Network fundamentals

- Module A: Network components
- Module B: Network addressing
- Module C: Network ports and applications

Chapter 5: Securing networks

- Module A: Network security components
- Module B: Transport encryption
- Module C: Hardening networks
- Module D: Monitoring and detection

Chapter 6: Securing hosts and data

- Module A: Securing hosts
- Module B: Securing data
- Module C: Mobile device security

Chapter 7: Securing network services

- Module A: Securing applications
- Module B: Virtual and cloud systems

Chapter 8: Authentication

- Module A: Authentication factors
- Module B: Authentication protocols

Chapter 9: Access control

- Module A: Access control principles
- Module B: Account management

Chapter 10: Organizational security

- Module A: Security policies
- Module B: User training
- Module C: Physical security and safety

Chapter 11: Disaster planning and recovery

- Module A: Business continuity
- Module B: Fault tolerance and recovery
- Module C: Incident response

CompTIA Cloud+ Prep

Course Overview

While IT professionals today are expected to understand some basic cloud terminology and concepts, and have likely worked with public cloud or Software-as-a-Service solutions, the ability to analyze, evaluate, design, and test cloud computing solutions are hard skills to find, and are in high demand. In this course, you will apply the skills required to evaluate and implement standard deployments. You will implement, maintain, and deliver cloud technologies including network, storage, and virtualization technologies to create cloud solutions. You will manage workload migrations, manage cloud vendors to control costs, use automation and orchestration to bring business value from cloud solutions, and ensure security of cloud implementations through the use of cybersecurity best practices. In addition, this course prepares you to pass the CompTIA® Cloud+® exam and earn the corresponding certification.

Course Objectives

In this course, you will deploy, test, secure, manage, optimize, and troubleshoot a cloud solution.
You will:

- Prepare to deploy cloud solutions.
- Deploy a pilot project.
- Test a pilot project deployment.
- Design a secure network for cloud deployment.
- Determine CPU and memory sizing for cloud deployments.
- Determine storage requirements for cloud deployments.
- Plan Identity and Access Management for cloud deployments.
- Analyze workload characteristics to ensure successful migration to the cloud.
- Secure systems to meet access requirements.
- Maintain cloud systems.
- Implement backup, restore, and business continuity measures.
- Analyze cloud systems for required performance.
- Analyze cloud systems for anomalies and growth forecasting.
- Troubleshoot deployment, capacity, automation, and orchestration issues.

- Troubleshoot connectivity issues.
- Troubleshoot security issues.

Course Outline

Lesson 1: Preparing to Deploy Cloud Solutions

Topic A: Describe Interaction of Cloud Components and Services
Topic B: Describe Interaction of Non-cloud Components and Services
Topic C: Evaluate Existing Components and Services for Cloud Deployment
Topic D: Evaluate Automation and Orchestration Options
Topic E: Prepare for Cloud Deployment

Lesson 2: Deploying a Pilot Project

Topic A: Manage Change in a Pilot Project
Topic B: Execute Cloud Deployment Workflow
Topic C: Complete Post-Deployment Configuration

Lesson 3: Testing Pilot Project Deployments

Topic A: Identify Cloud Service Components for Testing
Topic B: Test for High Availability and Accessibility
Topic C: Perform Deployment Load Testing
Topic D: Analyze Test Results

Lesson 4: Designing a Secure and Compliant Cloud Infrastructure

Topic A: Design Cloud Infrastructure for Security
Topic B: Determine Organizational Compliance Needs

Lesson 5: Designing and Implementing a Secure Cloud Environment

Topic A: Design Virtual Network for Cloud Deployment
Topic B: Determine Network Access Requirements
Topic C: Secure Networks for Cloud Interaction
Topic D: Manage Cloud Component Security
Topic E: Implement Security Technologies

Lesson 6: Planning Identity and Access Management for Cloud Deployments

Topic A: Determine Identity Management and Authentication Technologies
Topic B: Plan Account Management Policies for the Network and Systems
Topic C: Control Access to Cloud Objects
Topic D: Provision Accounts

Lesson 7: Determining CPU and Memory Sizing for Cloud Deployments

Topic A: Determine CPU Size for Cloud Deployment
Topic B: Determine Memory Size for Cloud Deployment

Lesson 8: Determining Storage Requirements for Cloud Deployments

Topic A: Determine Storage Technology Requirements

Topic B: Select Storage Options for Deployment
Topic C: Determine Storage Access and Provisioning Requirements
Topic D: Determine Storage Security Options

Lesson 9: Analyzing Workload Characteristics to Ensure Successful Migration
Topic A: Determine the Type of Cloud Deployment to Perform
Topic B: Manage Virtual Machine and Container Migration
Topic C: Manage Network, Storage, and Data Migration

Lesson 10: Maintaining Cloud Systems
Topic A: Patch Cloud Systems
Topic B: Design and Implement Automation and Orchestration for Maintenance

Lesson 11: Implementing Backup, Restore, Disaster Recovery, and Business Continuity Measures
Topic A: Back Up and Restore Cloud Data
Topic B: Implement Disaster Recovery Plans
Topic C: Implement Business Continuity Plans

Lesson 12: Analyzing Cloud Systems for Performance
Topic A: Monitor Cloud Systems to Measure Performance
Topic B: Optimize Cloud Systems to Meet Performance Criteria

Lesson 13: Analyzing Cloud Systems for Anomalies and Growth Forecasting
Topic A: Monitor for Anomalies and Resource Needs
Topic B: Plan for Capacity
Topic C: Create Reports on Cloud System Metrics

Lesson 14: Troubleshooting Deployment, Capacity, Automation, and Orchestration Issues
Topic A: Troubleshoot Deployment Issues
Topic B: Troubleshoot Capacity Issues
Topic C: Troubleshoot Automation and Orchestration Issues

Lesson 15: Troubleshooting Connectivity Issues
Topic A: Identify Connectivity Issues
Topic B: Troubleshoot Connectivity Issues

Lesson 16: Troubleshooting Security Issues
Topic A: Troubleshoot Identity and Access Issues
Topic B: Troubleshoot Attacks
Topic C: Troubleshoot Other Security Issues

Cisco CCNA v1.0 – Implementing and Administering Cisco

Course Overview

The Implementing and Administering Cisco Solutions (CCNA) v1.0 course gives you a broad range of fundamental knowledge for all IT careers. Through a combination of lecture and hands-on labs, you will learn how to install, operate, configure, and verify basic IPv4 and IPv6 networks. The course covers configuring network components such as switches, routers, and wireless LAN controllers; managing network devices; and identifying basic security threats. The course also gives you a foundation in network programmability, automation, and software-defined networking.

This course helps you prepare to take the 200-301 Cisco® Certified Network Associate (CCNA®) exam. By passing this one exam, you earn CCNA certification.

Course Objectives

- Identify the components of a computer network and describe their basic characteristics
- Understand the model of host-to-host communication
- Describe the features and functions of the Cisco Internetwork Operating System (IOS®) software
- Describe LANs and the role of switches within LANs
- Describe Ethernet as the network access layer of TCP/IP and describe the operation of switches
- Install a switch and perform the initial configuration
- Describe the TCP/IP Internet layer, IPv4, its addressing scheme, and subnetting
- Describe the TCP/IP Transport layer and Application layer
- Explore functions of routing
- Implement basic configuration on a Cisco router
- Explain host-to-host communications across switches and routers
- Identify and resolve common switched network issues and common problems associated with IPv4 addressing
- Describe IPv6 main features and addresses, and configure and verify basic IPv6 connectivity
- Describe the operation, benefits, and limitations of static routing
- Describe, implement, and verify virtual local area networks (VLANs) and trunks
- Describe the application and configuration of inter-VLAN routing
- Explain the basics of dynamic routing protocols and describe components and terms of Open Shortest Path First (OSPF)
- Explain how Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) work
- Configure link aggregation using EtherChannel
- Describe the purpose of Layer 3 redundancy protocols
- Describe basic WAN and VPN concepts
- Describe the operation of access control lists (ACLs) and their applications in the network
- Configure Internet access using Dynamic Host Configuration Protocol (DHCP) clients and explain and configure network address translation (NAT) on Cisco routers
- Describe basic quality of service (QoS) concepts

- Describe the concepts of wireless networks, which types of wireless networks can be built, and how to use Wireless LAN Controllers (WLCs)
- Describe network and device architectures and introduce virtualization
- Introduce the concept of network programmability and Software-Defined Networking (SDN) and describe smart network management solutions such as Cisco DNA Center™, Software-Defined Access (SD-Access), and Software-Defined Wide Area Network (SD-WAN)
- Configure basic IOS system monitoring tools
- Describe the management of Cisco devices
- Describe the current security threat landscape
- Describe threat defense technologies
- Implement a basic security configuration of the device management plane
- Implement basic steps to harden network devices

Course Outline

This class includes lecture sections and some self-study sections. In instructor-led classes, lectures are delivered in real-time, either in person or remote. The self-study sections are available online.

- Exploring the Functions of Networking
- Introducing the Host-to-Host Communications Model
- Operating Cisco IOS Software
- Introducing LANs
- Exploring the TCP/IP Link Layer
- Starting a Switch
- Introducing the TCP/IP Internet Layer, IPv4 Addressing, and Subnets
- Explaining the TCP/IP Transport Layer and Application Layer
- Exploring the Functions of Routing
- Configuring a Cisco Router
- Exploring the Packet Delivery Process
- Troubleshooting a Simple Network
- Introducing Basic IPv6
- Configuring Static Routing
- Implementing VLANs and Trunks
- Routing Between VLANs
- Introducing OSPF
- Building Redundant Switched Topologies (Self-study)
- Improving Redundant Switched Topologies with EtherChannel
- Exploring Layer 3 Redundancy (Self-study)
- Introducing WAN Technologies (Self-study)
- Explaining Basics of ACL
- Enabling Internet Connectivity
- Introducing QoS (Self-study)
- Explaining Wireless Fundamentals (Self-study)

- Introducing Architectures and Virtualization (Self-study)
- Explaining the Evolution of Intelligent Networks
- Introducing System Monitoring
- Managing Cisco Devices
- Examining the Security Threat Landscape (Self-study)
- Implementing Threat Defense Technologies (Self-study)
- Securing Administrative Access
- Implementing Device Hardening

Lab Outline

- Get Started with Cisco Command-Line Interface (CLI)
- Observe How a Switch Operates
- Perform Basic Switch Configuration
- Implement the Initial Switch Configuration
- Inspect TCP/IP Applications
- Configure an Interface on a Cisco Router
- Configure and Verify Layer 2 Discovery Protocols
- Implement an Initial Router Configuration
- Configure Default Gateway
- Explore Packet Forwarding
- Troubleshoot Switch Media and Port Issues
- Troubleshoot Port Duplex Issues
- Configure Basic IPv6 Connectivity
- Configure and Verify IPv4 Static Routes
- Configure IPv6 Static Routes
- Implement IPv4 Static Routing
- Implement IPv6 Static Routing
- Configure VLAN and Trunk
- Troubleshoot VLANs and Trunk
- Configure a Router on a Stick
- Implement Multiple VLANs and Basic Routing Between the VLANs
- Configure and Verify Single-Area OSPF
- Configure and Verify EtherChannel
- Improve Redundant Switched Topologies with EtherChannel
- Configure and Verify IPv4 ACLs
- Implement Numbered and Named IPv4 ACLs
- Configure a Provider-Assigned IPv4 Address
- Configure Static NAT
- Configure Dynamic NAT and Port Address Translation (PAT)
- Implement PAT
- Log into the WLC

- Monitor the WLC
- Configure a Dynamic (VLAN) Interface
- Configure a DHCP Scope
- Configure a WLAN
- Define a Remote Access Dial-In User Service (RADIUS) Server
- Explore Management Options
- Explore the Cisco DNA™ Center
- Configure and Verify NTP
- Configure System Message Logging
- Create the Cisco IOS Image Backup
- Upgrade Cisco IOS Image
- Configure WLAN Using Wi-Fi Protected Access 2 (WPA2) Pre-shared Key (PSK) Using the GUI
- Secure Console and Remote Access
- Enable and Limit Remote Access Connectivity
- Secure Device Administrative Access
- Configure and Verify Port Security
- Implement Device Hardening

ISC^2 Certified Cloud Security Professional

Course Overview

This course is the most comprehensive review of cloud security concepts and industry best practices covering the six domains of the CCSP Common Body of Knowledge (CBK®). You will gain knowledge in identifying the types of controls necessary to administer various levels of confidentiality, integrity, and availability, with regard to securing data in the cloud. You will identify the virtual and physical components of the cloud infrastructure with regard to risk management analysis, including tools and techniques necessary for maintaining a secure cloud infrastructure. You will gain an understanding in cloud software assurance and validation, utilizing secure software, and the controls necessary for developing secure cloud environments. You will identify privacy issues and audit processes utilized within a cloud environment, including auditing controls, assurance issues, and the specific reporting attributes.

This course provides in-depth coverage required to pass the CCSP exam:

1. Architectural concepts and design requirements
2. Cloud data security
3. Cloud platform and infrastructure security
4. Cloud application security
5. Operations
6. Legal and compliance

Course Outline

Chapter 1: Architectural Concepts
Chapter 2: Design Requirements
Chapter 3: Data Classification
Chapter 4: Cloud Data Security
Chapter 5: Security in the Cloud
Chapter 6: Responsibilities in the Cloud
Chapter 7: Cloud Application Security
Chapter 8: Operations Elements
Chapter 9: Operations Management
Chapter 10: Legal And Compliance, Part 1
Chapter 11: Legal And Compliance, Part 2

Preparation for Cybersecurity Professional

Distance Learning (Online) and Fort Walton Beach

This program is comprised of content drawn from 4 courses which are well-regarded within the IT security field, namely the CompTIA Security+, CompTIA Advanced Security Practitioner (CASP+), EC-Council Certified Ethical Hacker (CEH), and EC-Council Computer Hacking Forensic Investigator. Over the span of 120 clock hours, students will be exposed to the course curricula from these five certification courses, in preparation for successfully passing the certification exams for the four related courses.

Please note: In order to obtain the IT Industry certifications covered by the contents of this program, the graduate must sit for and pass the following exams:

- Exam Prep: SY0-501 (CompTIA Security+ Exam)
- Exam Prep: 312.50 (EC-Council Certified Ethical Hacker)
- Exam Prep: 312.49 (EC-Council Computer Hacking Forensic Investigator)
- Exam Prep: CAS-003 (CompTIA Advanced Security Practitioner)

Program Objective:
To obtain the CompTIA Security+, EC-Council Certified Ethical Hacker (CEH), EC-Council Computer Hacking Forensic Investigator (CHFI) and the CompTIA Advanced Security Practitioner (CASP) certifications.

Program Requirements:
A secondary degree (High School Diploma, Associates degree or global equivalent.) Proficiency using the Windows environment and general knowledge of Hardware and Network concepts coupled with a minimum of one year (12 months) of general computing experience is recommended.

COURSE TITLE	**CLOCK HOURS**
COMPT008 – CompTIA Security+ Certification	40
ICOEC006– EC-Council Certified Ethical Hacker Certification	40
ICOE007 – EC-Council Computer Hacking Forensic Investigator	40
COMPT0012 – CompTIA Advanced Security Practitioner	40
PROGRAM TOTAL	**160.0**

CompTIA Security+ Prep

Course Overview

This course will prepare students to pass the current CompTIA Security+ SY0-501 certification. After taking this course, students will understand the field of network security and how it relates to other areas of information technology. This course also provides the broad-based knowledge necessary to prepare for further study in specialized security fields, or it can serve as a capstone course that gives a general introduction to the field.

Course Objectives

Upon completion of this course, students will be able to:

- Identify security threats.
- Harden internal systems and services.
- Harden internetwork devices and services.
- Secure network communications.
- Manage a PKI.
- Manage certificates.
- Enforce an organizational security policy.
- Monitor the security infrastructure.

Instructional Methods

- Lecture
- Overhead slides
- Lab exercises

Course Outline

Chapter 1: Security Fundamentals

- Module A: Security concepts
- Module B: Risk management
- Module C: Vulnerability assessment

Chapter 2: Understanding attacks

- Module A: Understanding attackers
- Module B: Social engineering
- Module C: Malware
- Module D: Network attacks
- Module E: Application attacks

Chapter 3: Cryptography

- Module A: Cryptography concepts
- Module B: Public key infrastructure

Chapter 4: Network fundamentals

- Module A: Network components
- Module B: Network addressing
- Module C: Network ports and applications

Chapter 5: Securing networks
- Module A: Network security components
- Module B: Transport encryption
- Module C: Hardening networks
- Module D: Monitoring and detection

Chapter 6: Securing hosts and data
- Module A: Securing hosts
- Module B: Securing data
- Module C: Mobile device security

Chapter 7: Securing network services
- Module A: Securing applications
- Module B: Virtual and cloud systems

Chapter 8: Authentication
- Module A: Authentication factors
- Module B: Authentication protocols

Chapter 9: Access control
- Module A: Access control principles
- Module B: Account management

Chapter 10: Organizational security
- Module A: Security policies
- Module B: User training
- Module C: Physical security and safety

Chapter 11: Disaster planning and recovery
- Module A: Business continuity
- Module B: Fault tolerance and recovery
- Module C: Incident response

Certified Ethical Hacker v10

Course Overview

This class will immerse the students into an interactive environment where they will be shown how to scan, test, hack and secure their own systems. The lab intensive environment gives each student in-depth knowledge and practical experience with the current essential security systems. Students will begin by understanding how perimeter defenses work and then be lead into scanning and attacking their own networks, no real network is harmed. Students then learn how intruders escalate privileges and what steps can be taken to secure a system. Students will also learn about Intrusion Detection, Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus Creation. This course in its 10th iteration, is updated to provide you with the tools and techniques used by hackers and information

security professionals alike to break into any computer system. This course will immerse you in a "Hacker Mindset" to teach you how to think like a hacker and better defend against future attacks. It puts you in the driver's seat with a hands-on training environment employing a systematic ethical hacking process.

Acquired Skills

- Key issues plaguing the information security world, incident management process, and penetration testing
- Various types of footprinting, footprinting tools, and countermeasures
- Network scanning techniques and scanning countermeasures
- Enumeration techniques and enumeration countermeasures
- System hacking methodology, steganography, steganalysis attacks, and covering tracks
- Different types of Trojans, Trojan analysis, and Trojan countermeasures
- Working of viruses, virus analysis, computer worms, malware analysis procedure, and countermeasures
- Packet sniffing techniques and how to defend against sniffing
- Social Engineering techniques, identify theft, and social engineering countermeasures
- DoS/DDoS attack techniques, botnets, DDoS attack tools, and DoS/DDoS countermeasures
- Session hijacking techniques and countermeasures
- Different types of webserver attacks, attack methodology, and countermeasures
- Different types of web application attacks, web application hacking methodology, and countermeasures
- SQL injection attacks and injection detection tools
- Wireless Encryption, wireless hacking methodology, wireless hacking tools, and wi- security tools
- Mobile platform attack vector, android vulnerabilities, jailbreaking iOS, windows phone 8 vulnerabilities, mobile security guidelines, and tools
- Firewall, IDS and honeypot evasion techniques, evasion tools, and countermeasures
- Various cloud computing concepts, threats, attacks, and security techniques and tools
- Different types of cryptography ciphers, Public Key Infrastructure (PKI), cryptography attacks, and cryptanalysis tools
- Various types of penetration testing, security audit, vulnerability assessment, and penetration testing roadmap
- Perform vulnerability analysis to identify security loopholes in the target organization's network, communication infrastructure, and end systems.
- Different threats to IoT platforms and learn how to defend IoT devices securely

Course Detail

- Introduction to Ethical Hacking
- Footprinting and Reconnaissance
- Scanning Networks
- Enumeration
- Vulnerability Analysis

- System Hacking
- Malware Threats
- Sniffing
- Social Engineering
- Denial-of-Service
- Session Hijacking
- Evading IDS, Firewalls, and Honeypots
- Hacking Web Servers
- Hacking Web Applications
- SQL Injection
- Hacking Wireless Networks
- Hacking Mobile Platforms
- IoT Hacking
- Cloud Computing
- Cryptography

EC-Council Computer Hacking Forensic Investigator

Course Overview

EC-Council released the most advanced computer forensic investigation program in the world. This course covers major forensic investigation scenarios that enable students to acquire hands-on experience on various forensic investigation techniques and standard tools necessary to successfully carry-out a computer forensic investigation. Students will learn how to excel in digital evidence acquisition, handling, and forensically sound analysis. These skills will lead to successful prosecutions in various types of security incidents such as data breaches, corporate espionage, insider threats, and other intricate cases involving computer systems.

Acquired Skills

- The computer forensic investigation process and the various legal issues involved
- Evidence searching, seizing and acquisition methodologies in a legal and forensically sound manner
- Types of digital evidence, rules of evidence, digital evidence examination process, and electronic crime and digital evidence consideration by crime category
- Roles of the first responder, first responder toolkit, securing and evaluating electronic crime scene, conducting preliminary interviews, documenting electronic crime scene, collecting and preserving electronic evidence, packaging and transporting electronic evidence, and reporting the crime scene
- Setting up a computer forensics lab and the tools involved in it
- Various file systems and how to boot a disk
- Gathering volatile and non-volatile information from Windows
- Data acquisition and duplication rules
- Validation methods and tools required
- Recovering deleted files and deleted partitions in Windows, Mac OS X, and Linux

- Forensic investigation using AccessData FTK and EnCase
- Steganography and its techniques
- Steganalysis and image file forensics
- Password cracking concepts, tools, and types of password attacks
- Investigating password protected files
- Types of log capturing, log management, time synchronization, and log capturing tools
- Investigating logs, network traffic, wireless attacks, and web attacks
- Tracking emails and investigate email crimes
- Mobile forensics and mobile forensics software and hardware tools
- Writing investigative reports

Course Detail

1. Computer Forensics in Today's World
2. Computer Forensics Investigation Process
3. Searching and Seizing Computers
4. Digital Evidence
5. First Responder Procedures
6. Computer Forensics Lab
7. Understanding Hard Disks and File Systems
8. Windows Forensics
9. Data Acquisition and Duplication
10. Recovering Deleted Files and Deleted Partitions
11. Forensics Investigation Using AccessData FTK
12. Forensics Investigation Using EnCase
13. Steganography and Image File Forensics
14. Application Password Crackers
15. Log Capturing and Event Correlation
16. Network Forensics, Investigating Logs and Investigating Network Traffic
17. Investigating Wireless Attacks
18. Investigating Web Attacks
19. Tracking Emails and Investigating Email Crimes
20. Mobile Forensics
21. Investigative Reports
22. Becoming an Expert Witness

CompTIA Advanced Security Practitioner+ (CASP+)

Course Overview

The CompTIA Advanced Security Practitioner (CASP) Certification is a vendor-neutral credential. The CASP exam is an internationally targeted validation of advanced-level security skills and knowledge. While there is no required prerequisite, the CASP certification is intended to follow CompTIA Security+ or equivalent experience and has a technical, "hands-on" focus at the enterprise level.

The CASP exam will certify that the successful candidate has the technical knowledge and skills required to conceptualize, engineer, integrate and implement secure solutions across complex environments. The candidate will apply critical thinking and judgment across a broad spectrum of security disciplines to propose and implement sustainable security solutions that map to organizational strategies, translate business needs into security requirements, analyzes risk impact and respond to security incidents.

Acquired Skills

- Manage risk in the enterprise
- Integrate computing, communications, and business disciplines in the enterprise
- Use research and analysis to secure the enterprise
- Integrate advanced authentication and authorization techniques
- Implement cryptographic techniques
- Implement security controls for hosts
- Implement security controls for storage
- Analyze network security concepts, components, and architectures, and implement controls
- Implement security controls for applications
- Integrate hosts, storage, networks, and applications in a secure enterprise architecture
- Conduct vulnerability assessments
- Conduct incident and emergency responses

Course Detail

1. Managing Risk

- Identify the Importance of Risk Management
- Assess Risk
- Mitigate Risk
- Integrate Documentation into Risk Management

2. Integrating Computing, Communications, and Business Disciplines

- Facilitate Collaboration Across Business Units
- Secure Communications and Collaboration Solutions
- Implement Security Activities Throughout the Technology Life Cycle

3. Using Research and Analysis to Secure the Enterprise

- Determine Industry Trends and Effects on the Enterprise
- Analyze Scenarios to Secure the Enterprise

4. Integrating Advanced Authentication and Authorization Techniques

- Implement Authentication and Authorization Technologies
- Implement Advanced Identity Management

5. Implementing Cryptographic Techniques

- Describe Cryptographic Concepts
- Choose Cryptographic Techniques
- Choose Cryptographic Implementations

6. Implementing Security Controls for Hosts

- Select Host Hardware and Software
- Harden Hosts
- Virtualize Servers and Desktops
- Implement Cloud Augmented Security Services
- Protect Boot Loaders

7. Implementing Security Controls for Enterprise Storage

- Identify Storage Types and Protocols
- Implement Secure Storage Controls

8. Analyzing and Implementing Network Security

- Analyze Network Security Components and Devices
- Analyze Network-Enabled Devices
- Analyze Advanced Network Design
- Configure Controls for Network Security

9. Implementing Security Controls for Applications

- Identify General Application Vulnerabilities
- Identify Web Application Vulnerabilities
- Implement Application Security Controls

10. Integrating Hosts, Storage, Networks, and Applications in a Secure Enterprise Architecture

- Implement Security Standards in the Enterprise
- Select Technical Deployment Models
- Secure the Design of the Enterprise Infrastructure
- Secure Enterprise Application Integration Enablers

11. Conducting Vulnerability Assessments

- Select Vulnerability Assessment Methods
- Select Vulnerability Assessment Tools

12. Responding to and Recovering from Incidents

- Design Systems to Facilitate Incident Response
- Conduct Incident and Emergency Responses

Appendix A: Mapping Course Content to CompTIA Advanced Security Practitioner (CASP)

Labs

Lab 1: Integrate Documentation into Risk Management
Lab 2: Secure Communications and Collaboration Solutions
Lab 3: Analyze Scenarios to Secure the Enterprise
Lab 4: Implement Authentication and Authorization Technologies

Lab 5; Choose Cryptographic Techniques
Lab 6: Harden Hosts
Lab 7: Virtualize Servers and Desktops
Lab 8: Protect Boot Loaders
Lab 9: Implement Secure Storage Controls
Lab 10: Configure Controls for Network Security
Lab 11: Implement Application Security Controls
Lab 12: Select Vulnerability Assessment Tools
Lab 13: Design Systems to Facilitate Incident Response
Lab 14: Conduct Incident and Emergency Responses

Preparation for Advanced Cybersecurity Professional

Distance Learning (Online) and Fort Walton Beach

The Certified Authorization Professional (CAP) is an information security practitioner who advocates for security risk management in pursuit of information system authorization to support an organization's mission and operations in accordance with legal and regulatory requirements.

Adding the CISSP course is the most comprehensive review of information security concepts and industry best practices and focuses on the eight domains of the CISSP CBK (Common Body of Knowledge) that are covered in the CISSP exam. You will gain knowledge in information security that will increase your ability to successfully implement and manage security programs in any organization or government entity.

- Exam Prep: ISC^2 Certified Authorization Professional (CAP)
- Exam Prep: ISC^2 Certified Information System Security Professional (CISSP)

Program Objective:
The students will be trained to obtain the ISC^2 Certified Authorization Professional (CAP) and ISC^2 Certified Information System Security Professional (CISSP) certifications.

Program Requirements:
To qualify for the CAP you must have a minimum of two years of cumulative paid work experience in one or more of the seven domains of the CAP Common Body of Knowledge (CBK). Part-time work and internships may also count towards your experience. The CISSP course requires a cumulative minimum of five years of experience working in IT Infrastructure and Cybersecurity.

COURSE TITLE	CLOCK HOURS
CAP001 - ISC^2 Certified Authorization Professional Certification	40
CISSP002 - ISC^2 Certified Info. Systems Security Professional Certification	40
PROGRAM TOTAL	**80.0**

ISC^2 Certified Authorization Professional (CAP)

Course Overview
The Risk Management Framework (RMF) is used by security professionals who are responsible for assessing risk and establishing documentation for their IT systems. The CAP, Certified

Authorization Professional certification covers the RMF in great detail and is the only security certification under the DoD8570 Mandate that aligns to each of the RMF steps. This official ISC2 course provides students with in-depth coverage on the skills and concepts in the 7 domains including RMF, Security Categorization, Security Controls implementation, assessment, monitoring and authorization. This course is for IT Professionals interested in learning more about lifecycle cybersecurity risk management, as well as auditors, infosec/information assurance practitioners and program managers who have a minimum of 2 years full-time experience in one or more of the 7 domains covered in the CAP exam.

Acquired Skills

- Prepare for and pass the CAP Exam
- Define and implement a Risk Management Framework (RMF)
- Select, tailor and document security controls
- Prepare for security control assessment
- Perform ongoing security control assessments

Course Outline

Risk Management Framework (RMF)

- Describe the RMF
- Describe and distinguish between the RMF steps
- Identify roles and define responsibilities
- Understand and describe how the RMF process relates to the organizational structure
- Understand the relationship between the RMF and System Development Life Cycle (SDLC)
- Understand legal, regulatory and other security requirements

Categorization of Information Systems

- Categorize the system
- Describe the information system (including the security authorization boundaries)
- Register the system

Selection of Security Controls

- Identify and document (inheritable) controls
- Select, tailor and document security controls
- Develop security control monitoring strategy
- Review and approve security plan

Security Control Implementation

- Implement selected security controls
- Document security control implementation

Security Control Assessment

- Prepare for security control assessment
- Develop security control assessment plan
- Assess security control effectiveness
- Develop initial security assessment report (SAR)
- Review interim SAR and perform initial remediation actions
- Develop final SAR and optional addendum

Information System Authorization

- Develop plan of action and milestones (POAM) (e.g., resources, schedule, requirements)
- Assemble security authorization package
- Determine risk
- Determine the acceptability of risk
- Obtain security authorization decision

Monitoring of Security Controls

- Determine security impact of changes to system and environment
- Perform ongoing security control assessments (e.g., continuous monitoring, internal and external assessments)
- Conduct ongoing remediation actions (resulting from incidents, vulnerability scans, audits, vendor updates, etc.)
- Update key documentation (e.g., SP, SAR, POAM)
- Perform periodic security status reporting
- Perform ongoing risk determination and acceptance
- Decommission and remove system

ISC2 Certified Information Systems Security Professional (CISSP)

Course Overview

This course is the most comprehensive review of information security concepts and industry best practices and covers the eight domains of the official CISSP CBK (Common Body of Knowledge). Students will gain knowledge in information security that will increase their ability to successfully implement and manage security programs in any organization or government entity.

Acquired Skills

In-depth coverage of the eight domains required to pass the CISSP exam:

1. Security and Risk Management
2. Asset Security
3. Security Engineering
4. Communications and Network Security
5. Identity and Access Management
6. Security Assessment and Testing
7. Security Operations
8. Software Development Security

Course Outline

1. Security and Risk Management (e.g., Security, Risk, Compliance, Law, Regulations, Business Continuity)

- Understand and Apply Concepts of Confidentiality, Integrity, and Availability
- Apply Security Governance Principles
- Compliance
- Understand Legal and Regulatory Issues that Pertain to Information Security in a Global Context
- Develop and Implement Documented Security Policy, Standards, Procedures, and Guidelines
- Understand Business Continuity Requirements
- Contribute to Personnel Security Policies
- Understand and Apply Risk Management Concepts
- Understand and Apply Threat Modeling
- Integrate Security Risk Considerations into Acquisitions Strategy and Practice
- Establish and Manage Security Education, Training, and Awareness

2. Asset Security (Protecting Security of Assets)

- Classify Information and Supporting Assets
- Determine and Maintain Ownership
- Protect Privacy
- Ensure Appropriate Retention
- Determine Data Security Controls
- Establish Handling Requirements

3. Security Engineering (Engineering and Management of Security)

- Implement and Manage an Engineering Life Cycle Using Security Design Principles
- Understand Fundamental Concepts of Security Models
- Select Controls and Countermeasures Based Upon Information Systems Security Standards
- Understand the Security Capabilities of Information Systems
- Assess and Mitigate the Vulnerabilities of Security Architectures, Designs, and Solution Elements
- Assess and Mitigate Vulnerabilities in Web-based Systems

- Assess and Mitigate Vulnerabilities in Mobile Systems
- Assess and Mitigate Vulnerabilities in Embedded Devices and Cyber-Physical Systems
- Apply Cryptography
- Apply Secure Principles to Site and Facility Design
- Design and Implement Facility Security

4. Communications and Network Security (Designing and Protecting Network Security)
- Apply Secure Design Principles to Network Architecture
- Securing Network Components
- Design and Establish Secure Communication Channels
- Prevent or Mitigate Network Attacks

5. Identity and Access Management (Controlling Access and Managing Identity)
- Control Physical and Logical Access to Assets
- Manage Identification and Authentication of People and Devices
- Integrate Identity as a Service (IDaaS)
- Integrate Third-Party Identity Services
- Implement and Manage Authorization Mechanisms
- Prevent or Mitigate Access Control Attacks
- Manage the Identity and Access Provisioning Life Cycle

6. Security Assessment and Testing (Designing, Performing, and Analyzing Security Testing)
- Design and Validate Assessment and Test Strategies
- Conduct Security Control Testing
- Collect Security Process Data
- Conduct or Facilitate Internal and Third-Party Audits

7. Security Operations (e.g., Foundational Concepts, Investigations, Incident Management, Disaster Recovery)
- Understand and Support Investigations
- Understand Requirements for Investigation Types
- Conduct Logging and Monitoring Activities
- Secure the Provisioning of Resources through Configuration Management
- Understand and Apply Foundational Security Operations Concepts
- Employ Resource Protection Techniques
- Conduct Incident Response
- Operate and Maintain Preventative Measures
- Implement and Support Patch and Vulnerability Management
- Participate in and Understand Change Management Processes
- Implement Recovery Strategies
- Implement Disaster Recovery Processes
- Test Disaster Recovery Plan

- Participate in Business Continuity Planning
- Implement and Manage Physical Security
- Participate in Personnel Safety

8. Software Development Security (Understanding, Applying, and Enforcing Software Security)
    - Understand and Apply Security in the Software Development Life Cycle
    - Enforce Security Controls in the Development Environment
    - Assess the Effectiveness of Software Security
    - Assess Software Acquisition Security

Preparation for Linux Network Professional

Distance Learning (Online) and Fort Walton Beach

In the Linux Network Professional program, you will learn how to configure, manage and troubleshoot common wired and wireless networks. You'll also learn basic hardware, software, and networking skills necessary to function in an entry-level Linux role. A Linux network professional provides hands-on support and monitoring of critical internal and client systems. You will become an IT pro who will use Linux to manage everything from cars and smartphones to servers and supercomputers, as a vast number of enterprises use Linux in cloud, cybersecurity, mobile and web administration applications.

- Exam Prep: CompTIA Network+
- Exam Prep: CompTIA Linux+

Program Objective:
To obtain the CompTIA Network+ and CompTIA Linux+ certifications.

Program Requirements:
Secondary degree (High School Diploma, Associates degree or global equivalent.) One year of general computing experience is recommended.

	CLOCK HOURS
COURSE TITLE	
COMPT006 – CompTIA Network+ N10-007	40
COMPT005 – CompTIA Linux+ XKO-004	40
PROGRAM TOTAL	**80.0**

CompTIA Network+ Prep

Course Overview
This course is designed to provide network technicians and support staff with the foundation-level skills they need to install, operate, manage, maintain, and troubleshoot a corporate network.

Course Objectives
Upon completion of this course, students will be able to:

- Identify the basic components of network theory.
- Identify the major network communications methods.
- Identify network data delivery methods.
- List and describe network media and hardware components.
- Identify the major types of network implementations.
- Identify the components of a TCP/IP network implementation.
- List the major services deployed on TCP/IP networks.

- Identify characteristics of a variety of network protocols.
- Identify the components of a LAN implementation.
- Identify the components of a WAN implementation.
- Identify major issues and technologies in network security.
- Identify the components of a remote network implementation.
- Identify major issues and technologies in disaster recovery.
- Identify major data storage technologies and implementations.
- Identify the primary network operating systems.
- Identify major issues, models, tools, and techniques in network troubleshooting.

Instructional Methods

- Lecture
- Overhead slides
- Lab

Course Outline

Chapter 1: Fundamentals
- Module A: Networking concepts
- Module B: Classifying networks
- Module C: Network models
- Module D: The troubleshooting process

Chapter 2: Physical networks
- Module A: Connection technologies
- Module B: Network devices
- Module C: Copper media
- Module D: Optical media
- Module E: Ethernet standards

Chapter 3: TCP/IP networks
- Module A: IP addressing
- Module B: Core protocols
- Module C: Network ports and applications

Chapter 4: Internetworking
- Module A: Switching
- Module B: Routing

Chapter 5: Wireless LANs
- Module A: Wireless networks
- Module B: Wireless LAN standards

Chapter 6: Wide area networks
- Module A: Internet connections
- Module B: WAN infrastructure

Chapter 7: Cybersecurity principles
- Module A: Goals and threats
- Module B: Digital security
- Module C: Transport encryption

Chapter 8: Defending networks
- Module A: Network security components
- Module B: Network authentication systems
- Module C: Hardening networks

Chapter 9: Evolving network technologies
- Module A: Network convergence
- Module B: Virtual and cloud systems

Chapter 10: Network operations
- Module A: Monitoring and optimization
- Module B: Fault tolerance and disaster recovery
- Module C: Incident response

Chapter 11: Network planning
- Module A: Network policy design
- Module B: Network installation
- Module C: Maintenance and upgrades

CompTIA Linux+

Course Overview
The Official CompTIA® Linux+® courseware builds on your existing experience with systems operations and administration to provide you with the knowledge and skills required to configure, manage, operate, and troubleshoot a Linux environment by using security best practices, scripting, and automation. This course will also prepare you for the Exam XKO-004.

Course Objectives
In this course, you will configure, operate, and troubleshoot Linux systems.

You will learn to:
- Perform basic Linux tasks.
- Manage users and groups.
- Manage permissions and ownership.
- Manage storage.
- Manage files and directories.
- Manage kernel modules.
- Manage the Linux boot process.
- Manage system components.
- Manage devices.

- Manage networking.
- Manage packages and software.
- Secure Linux systems.
- Write and execute Bash shell scripts.
- Automate tasks.
- Plan and perform a Linux installation.

Course Outline

Lesson 1: Performing Basic Linux Tasks
Topic A: Identify the History and Development of Linux
Topic B: Enter Shell Commands
Topic C: Get Help Using Linux
Topic D: Start and Stop Linux

Lesson 2: Managing User and Group Accounts
Topic A: Create User and Group Accounts
Topic B: Configure User Profiles
Topic C: Administer User and Group Accounts

Lesson 3: Managing Partitions and the Linux Filesystem
Topic A: Create Partitions
Topic B: Navigate Through the Linux Filesystem
Topic C: Manage the Filesystem
Topic D: Maintain the Filesystem

Lesson 4: Managing Files in Linux
Topic A: Create and Edit Text Files
Topic B: Locate Files
Topic C: Search Text Using Regular Expressions
Topic D: Apply Filters to Text Streams
Topic E: Link Files
Topic F: Back Up and Restore Files
Topic G: Manage Databases Using MariaDB

Lesson 5: Managing Linux Permissions and Ownership
Topic A: Modify File and Directory Permissions
Topic B: Modify Default Permissions
Topic C: Modify File and Directory Ownership
Topic D: Set Special Permissions and Attributes

Lesson 6: Printing Files
Topic A: Configure a Local Printer
Topic B: Print Files
Topic C: Configure Remote Printing

Lesson 7: Managing Packages
Topic A: Manage Packages Using RPM

Topic B: Verify Packages
Topic C: Upgrade Packages
Topic D: Configure Repositories
Topic E: Manage Packages Using YUM
Topic F: Advanced Package and Application Management

Lesson 8: Managing Kernel Services
Topic A: Explore the Linux Kernel
Topic B: Customize Kernel Modules
Topic C: Create an initrd Image
Topic D: Manage Device Drivers and Hardware Devices
Topic E: Monitor Processes and Resources

Lesson 9: Working with the Bash Shell and Shell Scripts
Topic A: Perform Basic Bash Shell Operations
Topic B: Write a Bash Shell Script
Topic C: Customize the Bash Shell
Topic D: Redirect Standard Input and Output
Topic E: Use Control Statements in Shell Scripts

Lesson 10: Managing Jobs and Processes
Topic A: Manage Jobs and Background Processes
Topic B: Manage Processes Using the Process Table
Topic C: Delay and Detach Jobs
Topic D: Schedule Jobs
Topic E: Maintain the System Time

Lesson 11: Managing System Services
Topic A: Configure System Services
Topic B: Monitor System Logs
Topic C: Configure Security-Enhanced Linux (SELinux)

Lesson 12: Configuring Network Services
Topic A: Connect to a Network
Topic B: Configure Routes
Topic C: Configure Client Network Services
Topic D: Manage Remote Network Systems

Lesson 13: Configuring Basic Internet Services
Topic A: Configure Email Services
Topic B: Control Internet Services

Lesson 14: Securing Linux
Topic A: Implement Basic System Security
Topic B: Secure User Accounts

Lesson 15: Managing Hardware
Topic A: Identify Common Hardware Components and Resources

Topic B: Configure Removable Hardware
Topic C: Configure Disk Quotas

Lesson 16: Troubleshooting Linux Systems
Topic A: Troubleshoot System-Based Issues
Topic B: Troubleshoot Hardware Issues
Topic C: Troubleshoot Network Connection and Security Issues

Lesson 17: Installing Linux
Topic A: Prepare for Installation
Topic B: The Linux Boot Process
Topic C: Configure GRUB
Topic D: Install the Operating System

Lesson 18: Configuring the GUI
Topic A: Implement X
Topic B: Customize the Display Manager
Topic C: Enable Accessibility Settings in Linux

Preparation for Python Programming Professional

Distance Learning (Online) and Fort Walton Beach

This program will equip students to be able to recognize and write syntactically correct Python code, recognize data types supported by Python, and be able to recognize and write Python code that will logically solve a given problem. They will also be able to demonstrate their ability to accomplish coding tasks related to the basics of programming in the Python language and the fundamental notions and techniques used in object-oriented programming.

The Microsoft Certified Technology Associate – Python and the Python Institute's Certified Associate in Python Programming (PCAP) certifications show that the individual is familiar with general computer programming concepts like conditional execution, loops, Python programming language syntax, semantics, and the runtime environment, as well as with general coding techniques and object-oriented programming. Becoming PCAP certified ensures that the individual is fully acquainted with all the primary means provided by Python 3 to enable her/him to start her/his own studies, and to open a path to the developer's career.

- Exam Prep: Microsoft Certified Technology Associate – Python
- Exam Prep: Python Institute's Certified Associate in Python Programming (PCAP)

Program Objective:
To obtain the Microsoft Certified Technology Associate – Python and the Python Institute's Certified Associate in Python Programming (PCAP) certifications.

Program Requirements:
Secondary degree (High School Diploma, Associates degree or global equivalent.) One year of general computing experience is recommended. Familiarity with the Python programming language is helpful but not required.

	CLOCK HOURS
COURSE TITLE	
MICRO112 – Microsoft Introduction to Programming Using Python	40.0
PICAP001 – Python Institute's Certified Associate in Python Programming	40.0
PROGRAM TOTAL	**80.0**

Introduction to Python

Course Overview

This 5-day course introduces the student to the Python language. Upon completion of this class, the student will be able to write non-trivial Python programs dealing with a wide variety of subject matter domains. Topics include language components, working with a professional IDE, control flow constructs, strings, I/O, collections, classes, modules, and regular expressions. The course is supplemented with many hands-on labs, solutions, and code examples.

Acquired Skills

- Create working Python scripts following best practices
- Use Python data types appropriately
- Read and write files with both text and binary data
- Get familiar with the standard library and its work-saving modules
- Use statements and control structures
- Create professional Python applications to a basic level
- Learn to work with functions such as modules and classes
- Know when to use collections such as lists, dictionaries, and sets

Course Detail

1. An Introduction to Python

A Brief History of Python
Python Versions
Installing Python
Environment Variables
Executing Python from the Command Line
IDLE
Editing Python Files
Python Documentation
Getting Help
Dynamic Types
Python Reserved Words
Naming Conventions

2. Basic Python Syntax

Basic Syntax
Comments
String Values
String Methods

The format Method
String Operators
Numeric Data Types
Conversion Functions
Simple Input and Output
The % Method
The print Function

3. Language Components
Indenting Requirements
The if Statement
Relational Operators
Logical Operators
Bit Wise Operators
The while Loop
break and continue
The for Loop

4. Collections
Lists
Tuples
Sets
Dictionaries
Sorting Dictionaries
Copying Collections

5. Functions
Defining Your Own Functions
Parameters
Function Documentation
Keyword and Optional Parameters
Passing Collections to a Function
Variable Number of Arguments
Scope
Functions - "First Class Citizens"
Passing Functions to a Function
Mapping Functions in a Dictionary
Lambda
Inner Functions
Closures

6. Modules
Modules
Standard Modules - sys
Standard Modules - math
Standard Modules - time
The dir Function

7. Exceptions
Errors
Run Time Errors
The Exception Model
Exception Hierarchy
Handling Multiple Exceptions
raise
assert
Writing Your Own Exception Classes

8. Input and Output
Data Streams
Creating Your Own Data Streams
Access Modes
Writing Data to a File
Reading Data From a File
Additional File Methods
Using Pipes as Data Streams
Handling IO Exceptions
Working with Directories
Metadata
The pickle Module

9. Classes in Python
Classes in Python
Principles of Object Orientation
Creating Classes
Instance Methods
File Organization
Special Methods
Class Variables
Inheritance
Polymorphism
Type Identification

Custom Exception Classes

10. Regular Expressions
Simple Character Matches
Special Characters
Character Classes
Quantifiers
The Dot Character
Greedy Matches
Grouping
Matching at Beginning or End
Match Objects
Substituting
Splitting a String
Compiling Regular Expressions
Flags

PCAP Certified Associate in Python Programming

Course Overview
PCAP – Certified Associate in Python Programming certification shows that the individual is familiar with general computer programming concepts like conditional execution, loops, Python programming language syntax, semantics, and the runtime environment, as well as with general coding techniques and object-oriented programming.

Becoming PCAP certified ensures that the individual is fully acquainted with all the primary means provided by Python 3 to enable her/him to start her/his own studies, and to open a path to the developer's career.

Course Outline
Module 1: Control and Evaluations

Objectives covered by the module

- basic concepts: interpreting and the interpreter, compilation and the compiler, language elements, lexis, syntax and semantics, Python keywords, instructions, indenting
- literals: Boolean, integer, floating-point numbers, scientific notation, strings
- operators: unary and binary, priorities and binding
- numeric operators: ** * / % // + –
- bitwise operators: ~ & ^ | << >>
- string operators: * +
- Boolean operators: not and or

- relational operators (== != > >= < <=), building complex Boolean expressions
- assignments and shortcut operators
- accuracy of floating-point numbers
- basic input and output: input(), print(), int(), float(), str() functions
- formatting print() output with end= and sep= arguments
- conditional statements: if, if-else, if-elif, if-elif-else
- the pass instruction
- simple lists: constructing vectors, indexing and slicing, the len() function
- simple strings: constructing, assigning, indexing, slicing comparing, immutability
- building loops: while, for, range(), in, iterating through sequences
- expanding loops: while-else, for-else, nesting loops and conditional statements
- controlling loop execution: break, continue

Module 2: Data Aggregates

Objectives covered by the module

- strings in detail: ASCII, UNICODE, UTF-8, immutability, escaping using the \ character, quotes and apostrophes inside strings, multiline strings, copying vs. cloning, advanced slicing, string vs. string, string vs. non-string, basic string methods (upper(), lower(), isxxx(), capitalize(), split(), join(), etc.) and functions (len(), chr(), ord()), escape characters
- lists in detail: indexing, slicing, basic methods (append(), insert(), index()) and functions (len(), sorted(), etc.), del instruction, iterating lists with the for loop, initializing, in and not in operators, list comprehension, copying and cloning
- lists in lists: matrices and cubes
- tuples: indexing, slicing, building, immutability
- tuples vs. lists: similarities and differences, lists inside tuples and tuples inside lists
- dictionaries: building, indexing, adding and removing keys, iterating through dictionaries as well as their keys and values, checking key existence, keys(), items() and values() methods

Module 3: Functions and Modules

Objectives covered by the module

- defining and invoking your own functions and generators
- return and yield keywords, returning results, the None keyword, recursion
- parameters vs. arguments, positional keyword and mixed argument passing, default parameter values
- converting generator objects into lists using the list() function
- name scopes, name hiding (shadowing), the global keyword
- lambda functions, defining and using
- map(), filter(), reduce(), reversed(), sorted() functions and the sort() method
- the if operator
- import directives, qualifying entities with module names, initializing modules
- writing and using modules, the __name__ variable
- pyc file creation and usage

- constructing and distributing packages, packages vs. directories, the role of the __init__.py file
- hiding module entities
- Python hashbangs, using multiline strings as module documentation

Module 4: Classes, Objects, and Exceptions

Objectives covered by the module

- defining your own classes, superclasses, subclasses, inheritance, searching for missing class components, creating objects
- class attributes: class variables and instance variables, defining, adding and removing attributes, explicit constructor invocation
- class methods: defining and using, the self parameter meaning and usage
- inheritance and overriding, finding class/object components
- single inheritance vs. multiple inheritance
- name mangling
- invoking methods, passing and using the self argument/parameter
- the __init__ method
- the role of the __str__ method
- introspection: __dict__, __name__, __module__, __bases__ properties, examining class/object structure
- writing and using constructors
- hasattr(), type(), issubclass(), isinstance(), super() functions
- using predefined exceptions and defining your own ones
- the try-except-else-finally block, the raise statement, the except-as variant
- exceptions hierarchy, assigning more than one exception to one except branch
- adding your own exceptions to an existing hierarchy
- assertions
- the anatomy of an exception object
- input/output basics: opening files with the open() function, stream objects, binary vs. text files, newline character translation, reading and writing files, bytearray objects
- read(), readinto(), readline(), write(), close() methods

Preparation for Cisco Certified Network Administrator

Distance Learning (Online) and Fort Walton Beach

The CCNA program prepares you for today's associate-level job roles in IT technologies. CCNA includes network security and automation and programmability. The program has one certification that cover a broad range of fundamentals for IT careers, with one exam and one training course to help you prepare. The CCNA program will cover network fundamentals, network access, IP connectivity, IP services, security fundamentals and automation and programmability.

- Exam Prep: Cisco Implementing and Administering Cisco Solutions 200-301

Program Objective:
To obtain the Cisco Certified Network Administrator certification.

Program Requirements:
Secondary degree (High School Diploma, Associates degree or global equivalent.) One year of general computing experience is recommended. Knowledge of basic IP addressing, and network fundamentals is also recommended.

COURSE TITLE	**CLOCK HOURS**
CISCO200301 – Cisco Implementing and Administering Cisco Solutions	40.0
PROGRAM TOTAL	**40.0**

Cisco CCNA v1.0 – Implementing and Administering Cisco

Course Overview

The Implementing and Administering Cisco Solutions (CCNA) v1.0 course gives you a broad range of fundamental knowledge for all IT careers. Through a combination of lecture and hands-on labs, you will learn how to install, operate, configure, and verify basic IPv4 and IPv6 networks. The course covers configuring network components such as switches, routers, and wireless LAN controllers; managing network devices; and identifying basic security threats. The course also gives you a foundation in network programmability, automation, and software-defined networking.

This course helps you prepare to take the 200-301 Cisco® Certified Network Associate (CCNA®) exam. By passing this one exam, you earn CCNA certification.

Course Objectives

- Identify the components of a computer network and describe their basic characteristics
- Understand the model of host-to-host communication
- Describe the features and functions of the Cisco Internetwork Operating System (IOS®) software
- Describe LANs and the role of switches within LANs
- Describe Ethernet as the network access layer of TCP/IP and describe the operation of switches
- Install a switch and perform the initial configuration

- Describe the TCP/IP Internet layer, IPv4, its addressing scheme, and subnetting
- Describe the TCP/IP Transport layer and Application layer
- Explore functions of routing
- Implement basic configuration on a Cisco router
- Explain host-to-host communications across switches and routers
- Identify and resolve common switched network issues and common problems associated with IPv4 addressing
- Describe IPv6 main features and addresses, and configure and verify basic IPv6 connectivity
- Describe the operation, benefits, and limitations of static routing
- Describe, implement, and verify virtual local area networks (VLANs) and trunks
- Describe the application and configuration of inter-VLAN routing
- Explain the basics of dynamic routing protocols and describe components and terms of Open Shortest Path First (OSPF)
- Explain how Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) work
- Configure link aggregation using EtherChannel
- Describe the purpose of Layer 3 redundancy protocols
- Describe basic WAN and VPN concepts
- Describe the operation of access control lists (ACLs) and their applications in the network
- Configure Internet access using Dynamic Host Configuration Protocol (DHCP) clients and explain and configure network address translation (NAT) on Cisco routers
- Describe basic quality of service (QoS) concepts
- Describe the concepts of wireless networks, which types of wireless networks can be built, and how to use Wireless LAN Controllers (WLCs)
- Describe network and device architectures and introduce virtualization
- Introduce the concept of network programmability and Software-Defined Networking (SDN) and describe smart network management solutions such as Cisco DNA Center™, Software-Defined Access (SD-Access), and Software-Defined Wide Area Network (SD-WAN)
- Configure basic IOS system monitoring tools
- Describe the management of Cisco devices
- Describe the current security threat landscape
- Describe threat defense technologies
- Implement a basic security configuration of the device management plane
- Implement basic steps to harden network devices

Course Outline

This class includes lecture sections and some self-study sections. In instructor-led classes, lectures are delivered in real-time, either in person or remote. The self-study sections are available online.

- Exploring the Functions of Networking
- Introducing the Host-to-Host Communications Model
- Operating Cisco IOS Software
- Introducing LANs
- Exploring the TCP/IP Link Layer
- Starting a Switch
- Introducing the TCP/IP Internet Layer, IPv4 Addressing, and Subnets
- Explaining the TCP/IP Transport Layer and Application Layer
- Exploring the Functions of Routing
- Configuring a Cisco Router
- Exploring the Packet Delivery Process

- Troubleshooting a Simple Network
- Introducing Basic IPv6
- Configuring Static Routing
- Implementing VLANs and Trunks
- Routing Between VLANs
- Introducing OSPF
- Building Redundant Switched Topologies (Self-study)
- Improving Redundant Switched Topologies with EtherChannel
- Exploring Layer 3 Redundancy (Self-study)
- Introducing WAN Technologies (Self-study)
- Explaining Basics of ACL
- Enabling Internet Connectivity
- Introducing QoS (Self-study)
- Explaining Wireless Fundamentals (Self-study)
- Introducing Architectures and Virtualization (Self-study)
- Explaining the Evolution of Intelligent Networks
- Introducing System Monitoring
- Managing Cisco Devices
- Examining the Security Threat Landscape (Self-study)
- Implementing Threat Defense Technologies (Self-study)
- Securing Administrative Access
- Implementing Device Hardening

Lab Outline

- Get Started with Cisco Command-Line Interface (CLI)
- Observe How a Switch Operates
- Perform Basic Switch Configuration
- Implement the Initial Switch Configuration
- Inspect TCP/IP Applications
- Configure an Interface on a Cisco Router
- Configure and Verify Layer 2 Discovery Protocols
- Implement an Initial Router Configuration
- Configure Default Gateway
- Explore Packet Forwarding
- Troubleshoot Switch Media and Port Issues
- Troubleshoot Port Duplex Issues
- Configure Basic IPv6 Connectivity
- Configure and Verify IPv4 Static Routes
- Configure IPv6 Static Routes
- Implement IPv4 Static Routing
- Implement IPv6 Static Routing
- Configure VLAN and Trunk
- Troubleshoot VLANs and Trunk
- Configure a Router on a Stick
- Implement Multiple VLANs and Basic Routing Between the VLANs
- Configure and Verify Single-Area OSPF
- Configure and Verify EtherChannel
- Improve Redundant Switched Topologies with EtherChannel

- Configure and Verify IPv4 ACLs
- Implement Numbered and Named IPv4 ACLs
- Configure a Provider-Assigned IPv4 Address
- Configure Static NAT
- Configure Dynamic NAT and Port Address Translation (PAT)
- Implement PAT
- Log into the WLC
- Monitor the WLC
- Configure a Dynamic (VLAN) Interface
- Configure a DHCP Scope
- Configure a WLAN
- Define a Remote Access Dial-In User Service (RADIUS) Server
- Explore Management Options
- Explore the Cisco DNA™ Center
- Configure and Verify NTP
- Configure System Message Logging
- Create the Cisco IOS Image Backup
- Upgrade Cisco IOS Image
- Configure WLAN Using Wi-Fi Protected Access 2 (WPA2) Pre-shared Key (PSK) Using the GUI
- Secure Console and Remote Access
- Enable and Limit Remote Access Connectivity
- Secure Device Administrative Access
- Configure and Verify Port Security
- Implement Device Hardening

Preparation for Cisco Certified Network Enterprise Professional

Distance Learning (Online) and Fort Walton Beach

CCNP Enterprise certification proves your skills with enterprise networking solutions. To earn CCNP Enterprise certification, you pass two exams: one that covers core enterprise technologies and one enterprise concentration exam of your choice, so you can customize your certification to your technical area of focus. Students will learn enterprise infrastructure including dual-stack (IPv4 and IPv6) architecture, virtualization, infrastructure, network assurance, security, and automation. Electives focus on emerging and industry-specific topics such as network design, SD-WAN, wireless, and automation.

Elective Concentration Exam Prep (Choose **One**) include:

300-410 ENARSI	Implementing Cisco Enterprise Advanced Routing and Services (ENARSI)
300-415 ENSDWI	Implementing Cisco SD-WAN Solutions (SDWAN300)
300-420 ENSLD	Designing Cisco Enterprise Networks (ENSLD)
300-425 ENWLSD	Designing Cisco Enterprise Wireless Networks (ENWLSD)
300-430 ENWLSI	Implementing Cisco Enterprise Wireless Networks (ENWLSI)
300-435 ENAUTO	Implementing Automation for Cisco Enterprise Solutions (ENAUI)

- Exam: Cisco Implementing and Operating Cisco Network Core Technologies 350-401
- Exam Elective: Choose one of six Cisco exam electives; 300-410, 300-415, 300-420, 300-425, 300-430 or 300-435

Program Objective:
To obtain the Cisco CCNP Enterprise certification.

Program Requirements:
Secondary degree (High School Diploma, Associates degree or global equivalent.) Two to five years' experience implementing enterprise networking solutions is recommended.

COURSE TITLE	**CLOCK HOURS**
CISCO410 – Implementing & Operating Cisco Network Core Technologies	40.0
CISCOELECT – Cisco Elective Course Training	40.0
PROGRAM TOTAL	**80.0**

Cisco ENARSI - Implementing Cisco Enterprise Advanced Routing & Services

Exam Reference: Cisco 300410

Course Objectives

After taking this course, you should be able to:

- Describe information security concepts and strategies within the network
- Describe common TCP/IP, network application, and endpoint attacks
- Describe how various network security technologies work together to guard against attacks
- Implement access control on Cisco ASA appliance and Cisco Firepower Next-Generation Firewall
- Describe and implement basic email content security features and functions provided by Cisco Email Security Appliance
- Describe and implement web content security features and functions provided by Cisco Web Security Appliance
- Describe Cisco Umbrella® security capabilities, deployment models, policy management, and Investigate console
- Introduce VPNs and describe cryptography solutions and algorithms
- Describe Cisco secure site-to-site connectivity solutions and explain how to deploy Cisco Internetwork Operating System (Cisco IOS®) Virtual Tunnel Interface (VTI)-based point-to-point IPsec VPNs, and point-to-point IPsec VPN on the Cisco ASA and Cisco Firepower Next-Generation Firewall (NGFW)
- Describe and deploy Cisco secure remote access connectivity solutions and describe how to configure 802.1X and Extensible Authentication Protocol (EAP) authentication
- Provide basic understanding of endpoint security and describe Advanced Malware Protection (AMP) for Endpoints architecture and basic features
- Examine various defenses on Cisco devices that protect the control and management plane
- Configure and verify Cisco IOS software Layer 2 and Layer 3 data plane controls
- Describe Cisco Stealthwatch Enterprise and Stealthwatch Cloud solutions
- Describe basics of cloud computing and common cloud attacks and how to secure cloud environment

Course Outline

- Describing Information Security Concepts*
  - Information Security Overview
  - Assets, Vulnerabilities, and Countermeasures
  - Managing Risk
  - Vulnerability Assessment
  - Understanding Common Vulnerability Scoring System (CVSS)

- Describing Common TCP/IP Attacks*
  - Legacy TCP/IP Vulnerabilities
  - IP Vulnerabilities

- Internet Control Message Protocol (ICMP) Vulnerabilities
- TCP Vulnerabilities
- User Datagram Protocol (UDP) Vulnerabilities
- Attack Surface and Attack Vectors
- Reconnaissance Attacks
- Access Attacks
- Man-in-the-Middle Attacks
- Denial of Service and Distributed Denial of Service Attacks
- Reflection and Amplification Attacks
- Spoofing Attacks
- Dynamic Host Configuration Protocol (DHCP) Attacks

- Describing Common Network Application Attacks*
  - Password Attacks
  - Domain Name System (DNS)-Based Attacks
  - DNS Tunneling
  - Web-Based Attacks
  - HTTP 302 Cushioning
  - Command Injections
  - SQL Injections
  - Cross-Site Scripting and Request Forgery
  - Email-Based Attacks

- Describing Common Endpoint Attacks*
  - Buffer Overflow
  - Malware
  - Reconnaissance Attack
  - Gaining Access and Control
  - Gaining Access via Social Engineering
  - Gaining Access via Web-Based Attacks
  - Exploit Kits and Rootkits
  - Privilege Escalation
  - Post-Exploitation Phase
  - Angler Exploit Kit

- Describing Network Security Technologies
  - Defense-in-Depth Strategy
  - Defending Across the Attack Continuum
  - Network Segmentation and Virtualization Overview
  - Stateful Firewall Overview
  - Security Intelligence Overview
  - Threat Information Standardization
  - Network-Based Malware Protection Overview
  - Intrusion Prevention System (IPS) Overview

  - Next Generation Firewall Overview
  - Email Content Security Overview
  - Web Content Security Overview
  - Threat Analytic Systems Overview
  - DNS Security Overview
  - Authentication, Authorization, and Accounting Overview
  - Identity and Access Management Overview
  - Virtual Private Network Technology Overview
  - Network Security Device Form Factors Overview

- Deploying Cisco ASA Firewall
  - Cisco ASA Deployment Types
  - Cisco ASA Interface Security Levels
  - Cisco ASA Objects and Object Groups
  - Network Address Translation
  - Cisco ASA Interface Access Control Lists (ACLs)
  - Cisco ASA Global ACLs
  - Cisco ASA Advanced Access Policies
  - Cisco ASA High Availability Overview

- Deploying Cisco Firepower Next-Generation Firewall
  - Cisco Firepower NGFW Deployments
  - Cisco Firepower NGFW Packet Processing and Policies
  - Cisco Firepower NGFW Objects
  - Cisco Firepower NGFW Network Address Translation (NAT)
  - Cisco Firepower NGFW Prefilter Policies
  - Cisco Firepower NGFW Access Control Policies
  - Cisco Firepower NGFW Security Intelligence
  - Cisco Firepower NGFW Discovery Policies
  - Cisco Firepower NGFW IPS Policies
  - Cisco Firepower NGFW Malware and File Policies

- Deploying Email Content Security
  - Cisco Email Content Security Overview
  - Simple Mail Transfer Protocol (SMTP) Overview
  - Email Pipeline Overview
  - Public and Private Listeners
  - Host Access Table Overview
  - Recipient Access Table Overview
  - Mail Policies Overview
  - Protection Against Spam and Graymail
  - Anti-virus and Anti-malware Protection
  - Outbreak Filters
  - Content Filters

  - Data Loss Prevention
  - Email Encryption

- Deploying Web Content Security
  - Cisco Web Security Appliance (WSA) Overview
  - Deployment Options
  - Network Users Authentication
  - Secure HTTP (HTTPS) Traffic Decryption
  - Access Policies and Identification Profiles
  - Acceptable Use Controls Settings
  - Anti-Malware Protection

- Deploying Cisco Umbrella*
  - Cisco Umbrella Architecture
  - Deploying Cisco Umbrella
  - Cisco Umbrella Roaming Client
  - Managing Cisco Umbrella
  - Cisco Umbrella Investigate Overview and Concepts

- Explaining VPN Technologies and Cryptography
  - VPN Definition
  - VPN Types
  - Secure Communication and Cryptographic Services
  - Keys in Cryptography
  - Public Key Infrastructure

- Introducing Cisco Secure Site-to-Site VPN Solutions
  - Site-to-Site VPN Topologies
  - IPsec VPN Overview
  - IPsec Static Crypto Maps
  - IPsec Static Virtual Tunnel Interface
  - Dynamic Multipoint VPN
  - Cisco IOS FlexVPN

- Deploying Cisco IOS VTI-Based Point-to-Point IPsec VPNs
  - Cisco IOS VTIs
  - Static VTI Point-to-Point IPsec Internet Key Exchange (IKE) v2 VPN Configuration

- Deploying Point-to-Point IPsec VPNs on the Cisco ASA and Cisco Firepower NGFW
  - Point-to-Point VPNs on the Cisco ASA and Cisco Firepower NGFW
  - Cisco ASA Point-to-Point VPN Configuration
  - Cisco Firepower NGFW Point-to-Point VPN Configuration

- Introducing Cisco Secure Remote Access VPN Solutions

  - Remote Access VPN Components
  - Remote Access VPN Technologies
  - Secure Sockets Layer (SSL) Overview

- Deploying Remote Access SSL VPNs on the Cisco ASA and Cisco Firepower NGFW
  - Remote Access Configuration Concepts
  - Connection Profiles
  - Group Policies
  - Cisco ASA Remote Access VPN Configuration
  - Cisco Firepower NGFW Remote Access VPN Configuration

- Explaining Cisco Secure Network Access Solutions
  - Cisco Secure Network Access
  - Cisco Secure Network Access Components
  - AAA Role in Cisco Secure Network Access Solution
  - Cisco Identity Services Engine
  - Cisco TrustSec

- Describing 802.1X Authentication
  - 802.1X and Extensible Authentication Protocol (EAP)
  - EAP Methods
  - Role of Remote Authentication Dial-in User Service (RADIUS) in 802.1X Communications
  - RADIUS Change of Authorization

- Configuring 802.1X Authentication
  - Cisco Catalyst® Switch 802.1X Configuration
  - Cisco Wireless LAN Controller (WLC) 802.1X Configuration
  - Cisco Identity Services Engine (ISE) 802.1X Configuration
  - Supplicant 802.1x Configuration
  - Cisco Central Web Authentication

- Describing Endpoint Security Technologies*
  - Host-Based Personal Firewall
  - Host-Based Anti-Virus
  - Host-Based Intrusion Prevention System
  - Application Whitelists and Blacklists
  - Host-Based Malware Protection
  - Sandboxing Overview
  - File Integrity Checking

- Deploying Cisco Advanced Malware Protection (AMP) for Endpoints*
  - Cisco AMP for Endpoints Architecture
  - Cisco AMP for Endpoints Engines

  - Retrospective Security with Cisco AMP
  - Cisco AMP Device and File Trajectory
  - Managing Cisco AMP for Endpoints

- Introducing Network Infrastructure Protection*
  - Identifying Network Device Planes
  - Control Plane Security Controls
  - Management Plane Security Controls
  - Network Telemetry
  - Layer 2 Data Plane Security Controls
  - Layer 3 Data Plane Security Controls

- Deploying Control Plane Security Controls*
  - Infrastructure ACLs
  - Control Plane Policing
  - Control Plane Protection
  - Routing Protocol Security

- Deploying Layer 2 Data Plane Security Controls*
  - Overview of Layer 2 Data Plane Security Controls
  - Virtual LAN (VLAN)-Based Attacks Mitigation
  - Spanning Tree Protocol (STP) Attacks Mitigation
  - Port Security
  - Private VLANs
  - Dynamic Host Configuration Protocol (DHCP) Snooping
  - Address Resolution Protocol (ARP) Inspection
  - Storm Control
  - MACsec Encryption

- Deploying Layer 3 Data Plane Security Controls*
  - Infrastructure Antispoofing ACLs
  - Unicast Reverse Path Forwarding
  - IP Source Guard

- Deploying Management Plane Security Controls*
  - Cisco Secure Management Access
  - Simple Network Management Protocol Version 3
  - Secure Access to Cisco Devices
  - AAA for Management Access

- Deploying Traffic Telemetry Methods*
  - Network Time Protocol
  - Device and Network Events Logging and Export
  - Network Traffic Monitoring Using NetFlow

- Deploying Cisco Stealthwatch Enterprise*
  - Cisco Stealthwatch Offerings Overview
  - Cisco Stealthwatch Enterprise Required Components
  - Flow Stitching and Deduplication
  - Stealthwatch Enterprise Optional Components
  - Stealthwatch Enterprise and ISE Integration
  - Cisco Stealthwatch with Cognitive Analytics
  - Cisco Encrypted Traffic Analytics
  - Host Groups
  - Security Events and Alarms
  - Host, Role, and Default Policies

- Describing Cloud and Common Cloud Attacks*
  - Evolution of Cloud Computing
  - Cloud Service Models
  - Security Responsibilities in Cloud
  - Cloud Deployment Models
  - Common Security Threats in Cloud
  - Patch Management in the Cloud
  - Security Assessment in the Cloud

- Securing the Cloud*
  - Cisco Threat-Centric Approach to Network Security
  - Cloud Physical Environment Security
  - Application and Workload Security
  - Cloud Management and API Security
  - Network Function Virtualization (NFV) and Virtual Network Functions (VNF)
  - Cisco NFV Examples
  - Reporting and Threat Visibility in Cloud
  - Cloud Access Security Broker
  - Cisco CloudLock®
  - OAuth and OAuth Attacks

- Deploying Cisco Stealthwatch Cloud*
  - Cisco Stealthwatch Cloud for Public Cloud Monitoring
  - Cisco Stealthwatch Cloud for Private Network Monitoring
  - Cisco Stealthwatch Cloud Operations
- Describing Software-Defined Networking (SDN*)
  - Software-Defined Networking Concepts
  - Network Programmability and Automation
  - Cisco Platforms and APIs
  - Basic Python Scripts for Automation

* This section is self-study material that can be done at your own pace if you are taking the instructor-led version of this course.

Lab outline

- Configure Network Settings and NAT on Cisco ASA
- Configure Cisco ASA Access Control Policies
- Configure Cisco Firepower NGFW NAT
- Configure Cisco Firepower NGFW Access Control Policy
- Configure Cisco Firepower NGFW Discovery and IPS Policy
- Configure Cisco NGFW Malware and File Policy
- Configure Listener, Host Access Table (HAT), and Recipient Access Table (RAT) on Cisco Email Security Appliance (ESA)
- Configure Mail Policies
- Configure Proxy Services, Authentication, and HTTPS Decryption
- Enforce Acceptable Use Control and Malware Protection
- Examine the Umbrella Dashboard
- Examine Cisco Umbrella Investigate
- Explore DNS Ransomware Protection by Cisco Umbrella
- Configure Static VTI Point-to-Point IPsec IKEv2 Tunnel
- Configure Point-to-Point VPN between the Cisco ASA and Cisco Firepower NGFW
- Configure Remote Access VPN on the Cisco Firepower NGFW
- Explore Cisco AMP for Endpoints
- Perform Endpoint Analysis Using AMP for Endpoints Console
- Explore File Ransomware Protection by Cisco AMP for Endpoints Console
- Explore Cisco Stealthwatch Enterprise v6.9.3
- Explore Cognitive Threat Analytics (CTA) in Stealthwatch Enterprise v7.0
- Explore the Cisco Cloudlock Dashboard and User Security
- Explore Cisco Cloudlock Application and Data Security
- Explore Cisco Stealthwatch Cloud
- Explore Stealthwatch Cloud Alert Settings, Watchlists, and Sensors

Cisco ENSDWI – Implementing Cisco SD-WAN Solutions

Exam Reference: Cisco 300415

Course Objectives

After taking this course, you should be able to:

- Describe the Cisco SD-WAN overlay network and how modes of operation differ in legacy WAN versus SD-WAN
- Describe options for SD-WAN cloud and on-premises deployments, as well as how to deploy virtual vEdge and physical cEdge devices with Zero Touch Provisioning (ZTP) and device templates

- Describe best practices in WAN routing protocols, as well as how to configure and implement transport-side connectivity, service-side routing, interoperability, and redundancy and high availability
- Describe dynamic routing protocols and best practices in an SD-WAN environment, transport-side connectivity, service-side connectivity, and how redundancy and high availability are achieved in SD-WAN environments
- Explain how to migrate from legacy WAN to Cisco SD-WAN, including typical scenarios for data center and branch
- Explain how to perform SD-WAN Day 2 operations, such as monitoring, reporting, logging, and upgrading

Course Outline

- Cisco SD-WAN Overlay Network
    - Examining Cisco SD-WAN Architecture
- Cisco SD-WAN Deployment
    - Examining Cisco SD-WAN Deployment Options
    - Deploying Edge Devices
    - Deploying Edge Devices with Zero-Touch Provisioning
    - Using Device Configuration Templates
    - Redundancy, High Availability, and Scalability
- Cisco SD-WAN Routing Options
    - Using Dynamic Routing
    - Providing Site Redundancy and High Availability
    - Configuring Transport-Side Connectivity
- Cisco SD-WAN Policy Configuration
    - Reviewing Cisco SD-WAN Policy
    - Defining Advanced Control Policies
    - Defining Advanced Data Policies
    - Implementing Application-Aware Routing
    - Implementing Internet Breakouts and Network Address Translation (NAT)
- Cisco SD-WAN Migration and Interoperability
    - Examining Cisco SD-WAN Hybrid Scenarios
    - Performing a Migration
- Cisco SD-WAN Management and Operations
    - Performing Day-2 Operations
    - Performing Upgrades

Lab outline

- Deploying Cisco SD-WAN Controllers
- Adding a Branch Using Zero Touch Provisioning (ZTP)
- Deploying Devices Using Configuration Templates
- Configuring Controller Affinity

- Implementing Dynamic Routing Protocols on Service Side
- Implementing Transport Location (TLOC) Extensions
- Implementing Control Policies
- Implementing Data Policies
- Implementing Application-Aware Routing
- Implementing Internet Breakouts
- Migrating Branch Sites
- Performing an Upgrade

Cisco ENSLD – Designing Cisco Enterprise Networks

Exam Reference: Cisco 300420

Course Objectives

After taking this course, you should be able to:

- Design Enhanced Interior Gateway Routing Protocol (EIGRP) internal routing for the enterprise network
- Design Open Shortest Path First (OSPF) internal routing for the enterprise network
- Design Intermediate System to Intermediate System (IS-IS) internal routing for the enterprise network
- Design a network based on customer requirements
- Design Border Gateway Protocol (BGP) routing for the enterprise network
- Describe the different types and uses of Multiprotocol BGP (MP-BGP) address families
- Describe BGP load sharing
- Design a BGP network based on customer requirements
- Decide where the L2/L3 boundary will be in your Campus network and make design decisions
- Describe Layer 2 design considerations for Enterprise Campus networks
- Design a LAN network based on customer requirements
- Describe Layer 3 design considerations in an Enterprise Campus network
- Examine Cisco SD-Access fundamental concepts
- Describe Cisco SD-Access Fabric Design
- Design an Software-Defined Access (SD-Access) Campus Fabric based on customer requirements
- Design service provider-managed VPNs
- Design enterprise-managed VPNs
- Design a resilient WAN
- Design a resilient WAN network based on customer requirements
- Examine the Cisco SD-WAN architecture
- Describe Cisco SD-WAN deployment options
- Design Cisco SD-WAN redundancy
- Explain the basic principles of QoS
- Design Quality of Service (QoS) for the WAN

- Design QoS for enterprise network based on customer requirements
- Explain the basic principles of multicast
- Designing rendezvous point distribution solutions
- Describe high-level considerations when doing IP addressing design
- Create an IPv6 addressing plan
- Plan an IPv6 deployment in an existing enterprise IPv4 network
- Describe the challenges that you might encounter when transitioning to IPv6
- Design an IPv6 addressing plan based on customer requirements
- Describe Network APIs and protocols
- Describe Yet Another Next Generation (YANG), Network Configuration Protocol (NETCONF), and Representational State Transfer Configuration Protocol (RESTCONF)

Course Outline

- Designing EIGRP Routing
- Designing OSPF Routing
- Designing IS-IS Routing
- Designing BGP Routing and Redundancy
- Understanding BGP Address Families
- Designing the Enterprise Campus LAN
- Designing the Layer 2 Campus
- Designing the Layer 3 Campus
- Discovering the Cisco SD-Access Architecture
- Exploring Cisco SD-Access Fabric Design
- Designing Service Provider-Managed VPNs
- Designing Enterprise-Managed VPNs
- Designing WAN Resiliency
- Examining Cisco SD-WAN Architectures
- Cisco SD-WAN Deployment Design Considerations
- Designing Cisco SD-WAN Routing and High Availability
- Understanding QoS
- Designing LAN and WAN QoS
- Exploring Multicast with Protocol-Independent Multicast-Sparse Mode
- Designing Rendezvous Point Distribution Solutions
- Designing an IPv4 Address Plan
- Exploring IPv6
- Deploying IPv6
- Introducing Network APIs and Protocols
- Exploring YANG, NETCONF, RESTCONF, and Model-Driven Telemetry

Lab outline

- Designing Enterprise Connectivity
- Designing an Enterprise Network with BGP Internet Connectivity

- Designing an Enterprise Campus LAN
- Designing Resilient Enterprise WAN
- Designing QoS in an Enterprise Network
- Designing an Enterprise IPv6 Network

Cisco ENWLSD – Designing Cisco Enterprise Wireless Networks

Exam Reference: Cisco 300425

Course Objectives

After taking this course, you should be able to:

- Describe and implement a Cisco-recommended structured design methodology
- Describe and implement industry standards, amendments, certifications, and Requests For Comments (RFCs)
- Describe and implement Cisco enhanced wireless features
- Describe and implement the wireless design process
- Describe and implement specific vertical designs
- Describe and implement site survey processes
- Describe and implement network validation processes

Course Outline

- Describing and Implementing a Structured Wireless Design Methodology
    - Importance of Planning Wireless Design with a Structured Methodology
    - Cisco Structured Design Model
    - Cisco Design Guides and Cisco Validated Designs for Wireless Networks
    - Role of the Project Manager When Designing Wireless Networks
- Describing and Implementing Industry Protocols and Standards
    - Wireless Standards Bodies
    - Institute of Electrical and Electronics Engineers (IEEE) 802.11 Standard and Amendments
    - Wi-Fi Alliance (WFA) Certifications
    - Relevant Internet Engineering Task Force (IETF) Wireless RFCs
    - Practice Activity
- Describing and Implementing Cisco Enhanced Wireless Features
    - Hardware and Software Choices for a Wireless Network Design
    - Cisco Infrastructure Settings for Wireless Network Design
    - Cisco Enhanced Wireless Features
- Examining Cisco Mobility and Roaming
    - Mobility and Intercontroller Mobility in a Wireless Network
    - Optimize Client Roaming in a Wireless Network
    - Cisco Workgroup Bridge (WGB) and WGB Roaming in a Wireless Network
- Describing and Implementing the Wireless Design Process

    - Overview of Wireless Design Process
    - Meet with the Customer to Discuss the Wireless Network Design
    - Customer Information Gathering for a Wireless Network Design
    - Design the Wireless Network
    - Deployment of the Wireless Network
    - Validation and Final Adjustments of the Wireless Network
    - Wireless Network Design Project Documents and Deliverables
- Describing and Implementing Specific Vertical Designs
    - Designs for Wireless Applications
    - Wireless Network Design Within the Campus
    - Extend Wireless Networks to the Branch Sites
- Examining Special Considerations in Advanced Wireless Designs
    - High-Density Designs in Wireless Networks
    - Introducing Location and Cisco Connected Mobile Experiences (CMX) Concepts
    - Design for Location
    - FastLocate and HyperLocation
    - Bridges and Mesh in a Wireless Network Design
    - Redundancy and High Availability in a Wireless Network
- Describing and Implementing the Site Survey Processes
    - Site Survey Types
    - Special Arrangements Needed for Site Surveys
    - Safety Aspects to be Considered During Site Surveys
    - Site Survey Tools in Cisco Prime Infrastructure
    - Third-Party Site Survey Software and Hardware Tools
- Describing and Implementing Wireless Network Validation Processes
    - Post-installation Wireless Network Validation
    - Making Post-installation Changes to a Wireless Network
    - Wireless Network Handoff to the Customer
    - Installation Report

Lab outline

- Use Cisco Prime Infrastructure as a Design Tool
- Create a Predictive Site Survey with Ekahau Pro
- Perform a Live Site Survey Using Access Point on a Stick (APoS)
- Simulate a Post-installation Network Validation Survey

Cisco ENWLSI – Implementing Cisco Enterprise Wireless Networks

Exam Reference: Cisco 300430

Course Objectives

After taking this course, you should be able to:

- Implement network settings to provide a secure wireless network infrastructure
- Troubleshoot security issues as they relate to the wireless network infrastructure
- Implement a secure wireless client and troubleshoot wireless client connectivity issues
- Implement and troubleshoot QoS in wireless networks
- Implement and troubleshoot advanced capabilities in wireless network services

Course Outline

- Securing and Troubleshooting the Wireless Network Infrastructure
- Implementing and Troubleshooting Secure Client Connectivity
- Implementing and Troubleshooting Quality of Service (QoS) in Wireless Networks
- Implementing and Troubleshooting Advanced Wireless Network Services

Lab Outline

- Lab Familiarization (Base Learning Lab)
- Configure Secure Management Access for Cisco Wireless LAN Controllers (WLCs) and Access Points (APs)
- Add Network Devices and External Resources to Cisco Prime Infrastructure
- Capture a Successful AP Authentication
- Implement Authentication, Authorization, and Accounting (AAA) Services for Central Mode WLANs
- Implement AAA Services for FlexConnect Mode Wireless LANs (WLANs)
- Configure Guest Services in the Wireless Network
- Configure Bring Your Own Device (BYOD) in the Wireless Network
- Capture Successful Client Authentications
- Configure QoS in the Wireless Network for Voice and Video Services
- Configure Cisco Application Visibility and Control (AVC) in the Wireless Network
- Capture Successful QoS Traffic Marking in the Wireless Network
- Configure, Detect, and Locate Services on the Cisco CMX

Cisco ENAUTO – Automating Cisco Enterprise Solutions

Exam Reference: Cisco 300435

Course Objectives

After taking this course, you should be able to:

- Describe the various models and APIs of the Cisco IOS-XE platform to perform Day 0 operations, improve troubleshooting methodologies with custom tools, augment the Command-Line Interface (CLI) using scripts, and integrate various workflows using Ansible and Python
- Explain the paradigm shift of model-driven telemetry and the building blocks of a working solution

- Control the tools and APIs to automate Cisco DNA infrastructure managed by Cisco DNA Center™
- Demonstrate workflows (configuration, verification, health checking, and monitoring) using Python, Ansible, and Postman
- Explain Cisco SD-WAN solution components, implement a Python library that works with the Cisco SD-WAN APIs to perform configuration, inventory management, and monitoring tasks, and implement reusable Ansible roles to automate provisioning new branch sites on an existing Cisco SD-WAN infrastructure
- Manage the tools and APIs to automate Cisco Meraki managed infrastructure and demonstrate workflows (configuration, verification, health checking, monitoring) using Python, Ansible, and Postman

Course Outline

- Introducing Cisco SD-WAN Programmability
- Building Cisco SD-WAN Automation with Python
- Building Cisco SD-WAN Automation with Ansible
- Managing Configuration with Ansible and Network Automation and Programmability Abstraction Layer with Multivendor support (NAPALM)
- Implementing On-Box Programmability and Automation with Cisco IOS XE Software
- Implementing Model-Driven Telemetry
- Day 0 Provisioning with Cisco IOS-XE
- Automating Cisco Meraki
- Implementing Meraki Integration APIs
- Implementing Automation in Enterprise Networks
- Building Cisco DNA Center Automation with Python
- Automating Operations using Cisco DNA Center

Lab outline

- Perform Administrative Tasks Using the Cisco SD-WAN API
- Build, Manage, and Operate Cisco SD-WAN Programmatically
- Consume SD-WAN APIs Using the Uniform Resource Identifier (URI) Module
- Build Reports Using Ansible-Viptela Roles
- Manage Feature Templates with Ansible
- Use NAPALM to Configure and Verify Device Configuration
- Implement On-Box Programmability and Automation with Cisco IOS XE Software
- Use Python on Cisco IOS XE Software
- Implement Streaming Telemetry with Cisco IOS XE
- Implement Cisco Meraki API Automation
- Explore Cisco Meraki Integration APIs
- Explore Cisco Meraki Webhook Alerts

Preparation for Microsoft Modern Desktop Administrator Associate

Distance Learning (Online) and Fort Walton Beach

Modern Desktop Administrators deploy, configure, secure, manage, and monitor devices and client applications in an enterprise environment. Students will be taught to deploy Windows, manage devices and data, configure connectivity, maintain Windows, deploy and update operating systems, manage policies and profiles, manage and protect devices and manage apps and data.

- Exam Prep: Microsoft Windows 10 – MD-100
- Exam Prep: Microsoft Managing Modern Desktops – MD-101

Program Objective:
To obtain the Microsoft 365 Certified: Modern Desktop Administrator Associate certification.

Program Requirements:
Secondary degree (High School Diploma, Associates degree or global equivalent.) One year of general computing experience is recommended.

COURSE TITLE	**CLOCK HOURS**
MICROMD100 – Microsoft Windows 10	40.0
MICROMD101 – Managing Modern Desktops	40.0
PROGRAM TOTAL	**80.0**

Microsoft 365 Modern Desktop Administrator (MDA)

Exam # Reference: MD-100/MD-101

Course Overview

In this course, students will learn how to support and configure Windows 10 desktops in an organizational environment. Students will develop skills that include learning how to install, customize, and update Windows 10 operating systems. Students will learn how to managing storage, files, and devices as well as how to configure network connectivity for Windows 10. Students will also learn how to secure the Windows 10 OS and protect the data on the device. Finally, students will learn how to manage and troubleshoot Windows 10.

Part 2 of this course covers three central elements of Microsoft 365 enterprise administration – Microsoft 365 security management, Microsoft 365 compliance management, and Microsoft 365 device management. In Microsoft 365 security management, you will examine all the

common types of threat vectors and data breaches facing organizations today, and you will learn how Microsoft 365's security solutions address these security threats. You will be introduced to the Microsoft Secure Score, as well as to Azure Active Directory Identity Protection. You will then learn how to manage the Microsoft 365 security services, including Exchange Online Protection, Advanced Threat Protection, Safe Attachments, and Safe Links. Finally, you will be introduced to the various reports that monitor your security health. You will then transition from security services to threat intelligence; specifically, using the Security Dashboard and Advanced Threat Analytics to stay ahead of potential security breaches.

Course Objectives
Install and customize Windows 10
Configure Updates for Windows.
Configure devices and drivers for Windows.
Configure storage for Windows.
Configure network and remote management settings in Windows.
Configure and manage browsers and applications in Windows.
Configure account access and authentication.
Configure file and folder permissions.
Describe methods for securing Windows 10, common threats and methods for mitigating against them.
Troubleshoot Windows and application installations.
Troubleshoot hardware and driver issues.
Troubleshoot file issues and perform recoveries.

By actively participating in this course, you will learn about the following:

- Microsoft 365 Security Metrics
- Microsoft 365 Security Services
- Microsoft 365 Threat Intelligence
- Data Governance in Microsoft 365
- Archiving and Retention in Office 365
- Data Governance in Microsoft 365 Intelligence
- Search and Investigations
- Device Management
- Windows 10 Deployment Strategies
- Mobile Device Management

Course Outline – MD-100 Windows 10

Module 1: Installing Windows
This module covers installing the Windows 10 OS. Students will learn the different editions of Windows 10, requirements, and new features introduced. This module covers how to install the OS, as well as methods for migrations and upgrading. Students will also learn about common tools used in the deployment process.

Lessons
Introducing Windows 10
Windows 10 Editions and Requirements
Deployment Options
Upgrading to Windows 10
Deployment Tools
Lab : In-place upgrade of Win7 to Win 10
Lab : Migrating User Settings using USMT
After completing this module, students will be able to:
Understanding the different editions and features of Windows 10.
Understand the Windows 10 client installation options.
Practice installing Windows 10.
Migrate content using the User State Migration Tool.

Module 2: Post-installation Configuration and Personalization
This module covers common post-installation tasks in Windows 10. Students will learn how to customize the user interface, as well as using the control panel and settings app to configure common OS settings. This course will also introduce students to Windows PowerShell. This module will cover how device drivers work and how they work. Students will also be introduced to managing and configuring hardware peripherals such as printers.
Lessons
Configure and Customize the Windows Start Menu
Common Configuration Options
Advanced Configuration Methods
Managing Drivers and Devices
Lab : Using Settings App & Control Panel
Lab : Using Group Policy Objects
Lab : Using PowerShell to Configure Windows
Lab : Managing local and network printers
After completing this module, students will be able to:
Customize the Windows 10 UI
Configure device specific settings such as power plans and mobile device options.
Use the Windows control panel and setting app to configure settings.
Perform tasks using Windows PowerShell.
Describe concepts related to drivers.
Describe printer management concepts.

Module 3: Updating Windows in Windows 10
In this module, Students will learn about keeping Windows 10 up-to-date. Students will be introduced to the new Windows servicing model and how it applies to various scenarios. Students will learn the various different methods for updating Windows and applications, as well as managing updates using tools like group policy and Windows Update for Business.
Lessons
Windows Servicing Model

Updating Windows
Lab : Updating Windows 10
After completing this module, students will be able to:
Describe the Windows servicing model.
Configure Windows update settings.
Describe updating Windows using WSUS.
Describe updating Windows using Windows Update for Business.
Configure Windows update using group policy.

Module 4: Configuring Networking
In this module, Students will learn about networking concepts. This module will introduce to IPv4 and IPv6, and concepts like DNS. Students will learn how to configure network settings in Windows, as well as learn about wireless network technologies. The module will conclude with methods of managing Windows remotely.
Lessons
Configure IP Network Connectivity
Implement Name Resolution
Implement Wireless Network Connectivity
Remote Access Overview
Remote Management
Lab : Configuring Network Connectivity
Lab : Configuring and Testing Name Resolution
Lab : Remote Management
After completing this module, students will be able to:
Configure IP network connectivity.
Describe how name resolution works.
Describe remote access technologies like VPNs.
Configure Windows for remote management and access.

Module 5: Configuring Storage
This module covers storage configuration and management in Windows 10. Students will be introduced to local, cloud and virtual storage options. This course will also cover configuring storage on client devices and introduce storage spaces.
Lessons
Overview of storage options
Managing Local Storage
Maintaining Disks and Volumes
Managing Storage Spaces
Lab : Managing Storage
Lab : Compressing Folders
Lab : Enabling Disk Quotas
Lab : Creating a Storage Space
Lab : Synchronizing files with OneDrive
Describe the options and benefits of local, cloud, and virtual storage.

Configure OneDrive.
Configure local disk partitions and volumes.
Describe the capabilities and benefits of Storage spaces.

Module 6: Managing Apps in Windows 10
In this module, Students will be introduced to App management in Windows 10. This module will cover the different types of apps and supported installation methods. Students will learn how to install apps using manual and automated methods, as well as manage app delivery using the Windows Store. Finally, this module will cover the differences between Internet Explorer and Microsoft Edge.
Lessons
Providing Apps to Users
Managing Universal Windows Apps
Web Browsers in Windows 10
Lab : Sideloading an App
Lab : Installing and Updating Microsoft Store Apps
Lab : Configuring Internet Explorer Enterprise Mode
After completing this module, students will be able to:
Describe the different types of applications.
Install applications manually and using automated methods.
Manage application deployment using the Windows Store.
Learn about web browser features in Windows 10.

Module 7: Configuring Authorization & Authentication
This module introduces the tools and features of Windows 10 for authorizing access to Windows 10 clients. Students will learn about methods for how users sign-in to Windows 10. This module also covers restricting what users can or cannot do on a device through methods like UAC and account types.
Lessons
Authentication
Configuring User Account Control
Implementing Device Registration
Lab : Lab: Joining a Domain
Lab : Lab: Creating Security Policies
Lab : Lab: Configuring UAC
After completing this module, students will be able to:
Describe the different methods for securing data and the Windows 10 OS.
Describe the different types of user and service accounts.
Configure Windows Hello.
Configure user account control.

Module 8: Configuring Data Access and Usage
In this module, Students will learn about permissions. This module will cover considerations for

different files systems. Students will learn how to configure file and folder permissions as well as shared folders. The module will conclude with configuring settings through methods such as local and group policy.

Lessons

Overview of File Systems
Configuring and Managing File Access
Configuring and Managing Shared Folders
Lab : Creating, Managing, and Sharing a Folder
Lab : Using Conditions to Control Access and Effective Permissions
After completing this module, students will be able to:
Describe the differences and benefits of supported file systems.
Configure file and folder permissions.
Configure shared folders.
Secure Windows through local policy settings.

Module 9: Configuring Threat Protection and Advanced Security

This module introduces students to protecting devices from external threats. Students will learn about the different types of common threats. This module will teach students about using encryption, firewalls, and IPSec to help protect against threats. The module will conclude with how to configure and use Windows Defender and AppLocker.

Lessons

Malware and Threat Protection
Windows Defender
Connection Security Rules
Advanced Protection Methods
Lab : Lab: Configuring Windows Defender
Lab : Lab: Creating Firewall Rules
Lab : Lab: Creating Connection Security Rules
Lab : Lab: Using EFS
Lab : Lab: Using Bitlocker
Lab : Lab: Configuring AppLocker
After completing this module, students will be able to:
Identify common security threats .
Describe the methods by which you can mitigate these common security threats.
Describe the different methods of encryption.
Describe how Windows firewall can secure the device.
Describe the benefits of using IPSec.
Describe the different features of Windows Defender.
Describe the benefits of using AppLocker.

Module 10: Supporting the Windows 10 Environment

This module will cover the Windows 10 architecture and common environments. Students will be introduced to the various tools used in maintaining Windows. This module will also discuss

methodologies for effectively troubleshooting issues and how to proactively manage and optimize Windows 10.

Lessons

Windows Architecture
Support and Diagnostic Tools
Monitoring and Troubleshooting Computer Performance
Lab : Monitoring Events
Lab : Monitoring Reliability and Performance
After completing this module, students will be able to:
Describe the Windows architecture.
Describe key stages in troubleshooting.
Describe the purpose and benefits of the various tools in Windows.
Use monitoring tools to establish a performance baseline
Optimize performance on Windows 10 clients.

Module 11: Troubleshooting Files & Applications

This module helps students plan for file backup and recovery. Students will learn how to plan and configure data protection strategies and how to perform various file and system recovery methods. This module also includes common methods for troubleshooting application installation issues, compatibility issues, and resolving browser issues.

Lessons

File Recovery in Windows 10
Application Troubleshooting
Lab : Using File History to Recover Files
Lab : Troubleshooting Desktop Apps
Lab : Troubleshooting Application Compatibility Issues
Lab : Troubleshooting Microsoft Edge Issues
After completing this module, students will be able to:
Describe the different methods of file recovery.
Configure Windows 10 to support individual file and system recovery.
Recover a device using the Reset This PC function.
Solve application compatibility issues with the Application Compatibility Toolkit.
Troubleshoot common browser issues.

Module 12: Troubleshooting the OS

In this module, Students will learn how to troubleshoot startup and service issues related to the operating system. This module will teach the different startup and recovery options, and how to troubleshoot different Windows services.

Lessons

Troubleshooting Windows Startup
Troubleshooting Operating System Service Issues
Lab : Recovering using Reset This PC
Lab : Recovering using a Restore Point
After completing this module, students will be able to:

Describe the various methods identifying and recovering from startup issues.
Describe when to use the various advanced startup options.
Identify and disable a failed service.
Identify and mitigate common locked account scenarios.

Module 13: Troubleshooting Hardware and Drivers
This module introduces hardware troubleshooting. Students will learn about driver management and how to troubleshoot devices. Students will also learn steps for troubleshooting system hardware and external peripherals such as USB drives and printers, including diagnostic methods and remediation.
Lessons
Troubleshooting Device Driver Failures
Overview of Hardware Troubleshooting
Troubleshooting Physical Failures
Lab : Recovering using Driver Rollback
After completing this module, students will be able to:
Troubleshoot and remediate driver issues.
Troubleshoot Peripherals
Diagnose and replace hardware.

Course Outline – MD-101 Managing Modern Desktops

Module 1: Introduction to Microsoft 365 Security Metrics
Lessons
Threat Vectors and Data Breaches
Security Solutions in Microsoft 365
Introduction to the Secure Score
Introduction to Azure Active Directory Identity Protection

Module 2: Managing Your Microsoft 365 Security Services
Lessons
Introduction to Exchange Online Protection
Introduction to Advanced Threat Protection
Managing Safe Attachments
Managing Safe Links
Monitoring and Reports

Module 3: Lab 1 - Manage Microsoft 365 Security Services
Lab : Manage Microsoft 365 Security Services
Exercise 1 - Set up a Microsoft 365 Trial Tenant
Exercise 2 - Implement an ATP Safe Links policy and Safe Attachment policy

Module 4: Microsoft 365 Threat Intelligence
Lessons

Overview of Microsoft 365 Threat Intelligence
Using the Security Dashboard
Configuring Advanced Threat Analytics

Module 5: Lab 2 - Implement Alert Notifications Using the Security Dashboard

Lab : Implement Alert Notifications Using the Security Dashboard
Exercise 1 - Prepare for implementing Alert Policies
Exercise 2 - Implement Security Alert Notifications
Exercise 3 - Implement Group Alerts
Exercise 4 - Implement eDiscovery Alerts

Module 6: Introduction to Data Governance in Microsoft 365

Lessons

Introduction to Archiving in Microsoft 365
Introduction to Retention in Microsoft 365
Introduction to Information Rights Management
Introduction to Secure Multipurpose Internet Mail Extension
Introduction to Office 365 Message Encryption
Introduction to Data Loss Prevention

Module 7: Archiving and Retention in Office 365

Lessons

In-Place Records Management in SharePoint
Archiving and Retention in Exchange
Retention Policies in the SCC

Module 8: Lab 3 - Implement Archiving and Retention

Lab : Implement Archiving and Retention
Exercise 1 - Initialize Compliance in Your Organization
Exercise 2 - Configure Retention Tags and Policies
Exercise 3 - Implement Retention Policies

Module 9: Implementing Data Governance in Microsoft 365 Intelligence

Lessons

Planning Your Security and Compliance Needs
Building Ethical Walls in Exchange Online
Creating a Simple DLP Policy from a Built-in Template
Creating a Custom DLP Policy
Creating a DLP Policy to Protect Documents
Working with Policy Tips

Module 10: Lab 4 - Implement DLP Policies

Lab : Implement DLP Policies
Exercise 1 - Manage DLP Policies

Exercise 2 - Test MRM and DLP Policies

Module 11: Managing Data Governance in Microsoft 365
Lessons
Managing Retention in Email
Troubleshooting Data Governance
Implementing Azure Information Protection
Implementing Advanced Features of AIP
Implementing Windows Information Protection

Module 12: Lab 5 - Implement AIP and WIP
Lab : Implement AIP and WIP
Exercise 1 - Implement Azure Information Protection
Exercise 2 - Implement Windows Information Protection

Module 13: Managing Search and Investigations
Lessons
Searching for Content in the Security and Compliance Center
Auditing Log Investigations
Managing Advanced eDiscovery

Module 14: Lab 6 - Manage Search and Investigations
Lab : Manage Search and Investigations
Exercise 1 - Investigate Your Microsoft 365 Data
Exercise 2 - Configure and Deploy a Data Subject Request

Module 15: Planning for Device Management
Lessons
Introduction to Co-management
Preparing Your Windows 10 Devices for Co-management
Transitioning from Configuration Manager to Intune
Introduction to Microsoft Store for Business
Planning for Mobile Application Management

Module 16: Lab 7 - Implement the Microsoft Store for Business
Lab : Implement the Microsoft Store for Business
Exercise 1 - Configure the Microsoft Store for Business
Exercise 2 - Manage the Microsoft Store for Business

Module 17: Planning Your Windows 10 Deployment Strategy
Lessons
Windows 10 Deployment Scenarios
Implementing Windows Autopilot
Planning Your Windows 10 Subscription Activation Strategy

Resolving Windows 10 Upgrade Errors
Introduction to Windows Analytics

Module 18: Implementing Mobile Device Management

Planning Mobile Device Management
Deploying Mobile Device Management
Enrolling Devices to MDM
Managing Device Compliance

Module 19: Lab 8 - Manage Devices with Intune
Lab : Manage Devices with Intune
Exercise 1 - Enable Device Management
Exercise 2 - Configure Azure AD for Intune
Exercise 3 - Create Intune Policies
Exercise 4 - Enroll a Windows 10 Device
Exercise 5 - Manage and Mon

Preparation for Microsoft 365 and Azure Security Administrator Associate

Distance Learning (Online) and Fort Walton Beach

Microsoft 365 technical tasks that are trained: implement and manage identity and access; implement and manage threat protection; implement and manage information protection; and manage governance and compliance features in Microsoft 365. Students are then equipped to manage cloud services that span storage, security, networking, and compute cloud capabilities. They will be taught a deep understanding of each service across the full IT lifecycle, and take requests for infrastructure services, applications, and environments. They will be able to make recommendations on services for optimal performance and scale, as well as provision, size, monitoring and then adjusting resources as appropriate.

- Exam Prep: Microsoft 365 Security Administration MS-500
- Exam Prep: Microsoft Azure Administrator AZ-103

Program Objective:
To obtain the Microsoft Azure Administrator Associate certification.

Program Requirements:
Secondary degree (High School Diploma, Associates degree or global equivalent.) One year of general computing experience is recommended.

COURSE TITLE	CLOCK HOURS
MICROMS500 – Microsoft 365 Security Administration MS-500	40.0
MICROAZ103 – Microsoft Azure Administrator Associate	40.0
PROGRAM TOTAL	**80.0**

Microsoft 365 Security Administrator

Exam # Reference: MS-500

Course Objectives

After completing this course, students should be able to:

- Administer user and group security in Microsoft 365.
- Manage passwords in Microsoft 365.
- Describe Azure Identity Protection features.
- Plan and implement Azure AD Connect.
- Manage synchronized identities.
- Plan implement federated identities.
- Describe and use conditional access.

- Describe cyber-attack threat vectors.
- Describe security solutions for Microsoft 365
- Use Microsoft Secure Score to evaluate your security posture.
- Use the Security Dashboard in the Microsoft Security & Compliance center.
- Configure various advanced threat protection services for Microsoft 365.
- Configure Advanced Threat Analytics.
- Plan and deploy Mobile Device Management.
- Implement information rights management.
- Secure messages in Office 365.
- Configure Data Loss Prevention policies.
- Deploy and manage Cloud App Security.
- Implement Azure information protection for Microsoft 365.
- Implement Windows information protection for devices.
- Plan and deploy a data archiving and retention system.
- Perform assessments in Compliance Manager.
- Manage email retention through Exchange.
- Conduct an audit log investigation.
- Create and manage an eDiscovery investigation.
- Manage GDPR data subject requests.

Course Outline

1 - User and Group Security

- User Accounts in Microsoft 365
- Administrator Roles and Security Groups in Microsoft 365
- Password Management in Microsoft 365
- Azure AD Identity Protection

2 - Identity Synchronization

- Introduction to Identity Synchronization
- Planning for Azure AD Connect
- Implementing Azure AD Connect
- Managing Synchronized Identities

3 - Federated Identities

- Introduction to Federated Identities
- Planning an AD FS Deployment
- Implementing AD FS

4 - Access Management

- Conditional Access

- Managing Device Access
- Role Based Access Control (RBAC)
- Solutions for External Access

5 - Security in Microsoft 365
- Threat Vectors and Data Breaches
- Security Solutions for Microsoft 365
- Microsoft Secure Score

6 - Advanced Threat Protection
- Exchange Online Protection
- Office 365 Advanced Threat Protection
- Managing Safe Attachments
- Managing Safe Links
- Azure Advanced Threat Protection
- Windows Defender Advanced Threat Protection

7 - Threat Intelligence
- Microsoft 365 Threat Intelligence
- Using the Security Dashboard
- Configuring Advanced Threat Analytics

8 - Mobility
- Plan for Mobile Application Management
- Plan for Mobile Device Management
- Deploy Mobile Device Management
- Enroll Devices to Mobile Device Management

9 - Information Protection
- Information Rights Management
- Secure Multipurpose Internet Mail Extension
- Office 365 Message Encryption
- Azure Information Protection
- Advanced Information Protection
- Windows Information Protection

10 - Data Loss Prevention
- Data Loss Prevention Explained
- Data Loss Prevention Policies
- Custom DLP Policies
- Creating a DLP Policy to Protect Documents

- Policy Tips

11 - Cloud Application Security
- Cloud Application Security Explained
- Using Cloud Application Security Information
- Office 365 Cloud App Security

12 - Archiving and Retention
- Archiving in Microsoft 365
- Retention in Microsoft 365
- Retention Policies in the Security and Compliance Center
- Archiving and Retention in Exchange
- In-place Records Management in SharePoint

13 - Data Governance in Microsoft 365
- Planning Security and Compliance Needs
- Building Ethical Walls in Exchange Online
- Manage Retention in Email
- Troubleshooting Data Governance
- Analytics and Telemetry

14 - Managing Search and Investigations
- Searching for Content in the Security and Compliance Center
- Audit Log Investigations
- Advanced eDiscovery

Microsoft Azure Administrator

Exam # Reference: AZ-103

Course Objectives

After completing this course, students will be able to:

- Implement access management with Azure users, groups, and role-based access control.
- Use Azure Monitor to configure Azure alerts and review the Azure Activity Log.
- Query and analyze Log Analytics data.
- Deploy resources with ARM templates and organize Azure resources.
- Optimize your use of Azure tools like the Azure portal, Azure PowerShell, Cloud Shell and the Azure CLI.
- Create Azure storage accounts for different data replication, pricing, and content scenarios.
- Implement virtual machine storage, blob storage, Azure files, and structured storage.

- Secure and manage storage with shared access keys, Azure backup, and Azure File Sync.
- Store and access data using Azure Content Delivery Network, and the Import and Export service.
- Explain virtual machine usage cases, storage options, pricing, operating systems, networking capabilities, and general planning considerations.
- Create Windows virtual machines in the Azure Portal, with Azure PowerShell, or using ARM Templates.
- Deploy custom server images and Linux virtual machines.
- Configure virtual machine networking and storage options.
- Implement virtual machine high availability, scalability, and custom scripts extensions.
- Backup, restore, and monitor virtual machines.
- Understand virtual networking components, IP addressing, and network routing options.
- Implement Azure DNS domains, zones, record types, and resolution methods.
- Configure network security groups, service endpoints, logging, and network troubleshooting.
- Implement site connectivity schemas including VNet-to-VNet connections and virtual network peering.
- Implement Azure Active Directory, Self-Service Password Reset, Azure AD Identity Protection, and integrated SaaS applications.
- Configure domains and tenants, users and groups, roles, and devices.
- Implement and manage Azure Active Directory integration options and Azure AD Application Proxy.
- Implement and configure Azure Load Balancer, Azure Traffic Manager, and Azure Application Gateway.
- Use Azure RBAC to grant a granular level of access based on an administrator's assigned tasks.
- Use Azure Multi-Factor Authentication to configure a strong authentication for users at sign-in.

Course Outline

Module 1: Azure Administration
In this module, you'll learn about the tools Azure Administrators use to manage their infrastructure. This includes the Azure Portal, Cloud Shell, Azure PowerShell, CLI, Resource Manager, and Resource Manager Templates. The demonstrations in this module will ensure you are successful in the course labs.
Lessons

- Azure Portal and Cloud Shell
- Azure PowerShell and CLI
- Resource Manager
- ARM Templates

Module 2: Azure Virtual Machines
In this module, you'll learn about Azure virtual machines including planning, creating, availability and extensions.
Lessons

- Virtual Machine Planning
- Creating Virtual Machines
- Virtual Machine Availability
- Virtual Machine Extensions

Module 3: Azure Storage
In this module, you'll learn about basic storage features including storage accounts, blob storage, Azure files, and storage security.
Lessons

- Storage Accounts
- Azure Blobs
- Azure Files
- Storage Security

Module 4: Virtual Networking
In this module, you'll learn about basic virtual networking concepts like virtual networks, IP addressing, Azure DNS, and network security groups.
Lessons

- Virtual Networks
- IP Addressing and Endpoints
- Azure DNS
- Network Security Groups

Module 5: Intersite Connectivity
In this module, you'll learn about intersite connectivity features including VNet Peering, VNet-to-VNet connections, Site-to-Site Connections, and ExpressRoute.

Lessons

- VNet Peering
- VNet-to-VNet Connections
- ExpressRoute Connections

Module 6: Monitoring
In this module, you'll learn about monitoring your Azure infrastructure including Azure Monitor, alerting, log analytics, and Network Watcher.
Lessons

- Azure Monitor
- Azure Alerts
- Log Analytics

- Network Watcher

Module 7: Data Protection
In this module, you'll learn about data replication strategies, backing up files and folders, and virtual machine backups.
Lessons

- Data Replication
- File and Folder Backups
- Virtual Machine Backups

Module 8: Network Traffic Management
In this module, you'll learn about network traffic strategies including service endpoints, network routing, Azure Load Balancer, and Azure Traffic Manager.
Lessons

- Network Routing
- Azure Load Balancer
- Azure Traffic Manager

Module 9: Azure Active Directory
In this module, you'll learn about Azure Active Directory (AD) including Azure AD Connect and Azure AD Join.
Lessons

- Azure Active Directory
- Azure AD Connect
- Azure AD Join

Module 10: Securing Identities
In this module, you'll learn how to secure identities including Multi-Factor Authentication, Azure AD Identity Protection, and Self-Service Password Reset
Lessons

- Multi-Factor Authentication
- Azure AD Identity Protection
- Self-Service Password Reset

Module 11: Governance and Compliance
In this module, you'll learn about managing your subscriptions and accounts including role-based access control, users and groups, and Azure policy.
Lessons

- Subscriptions and Accounts
- Role-Based Access Control (RBAC)
- Users and Groups
- Azure Policy

Module 12: Data Services

In this module, you'll learn how to effectively share data using Import and Export service, Data Box Content Delivery Network, and File Sync.

Lessons

- Content Delivery Network
- File Sync
- Import and Export Service
- Data Box

Preparation for Microsoft Enterprise Administrator Expert

Distance Learning (Online) and Fort Walton Beach

Microsoft 365 Enterprise Administrators evaluate, plan, migrate, deploy, and manage Microsoft 365 services. Students will be able to demonstrate the ability to perform Microsoft 365 tenant management tasks for an enterprise, including its identities, security, compliance, and supporting technologies.

- Exam Prep: Microsoft 365 Identity and Services MS-100
- Exam Prep: Microsoft 365 Mobility and Security MS101

Program Objective:
To obtain the Microsoft 365 Certified: Enterprise Administrator Expert certification.

Program Requirements:
Secondary degree (High School Diploma, Associates degree or global equivalent.) One year of general computing experience is recommended.

COURSE TITLE	CLOCK HOURS
MICROMS100 – Microsoft 365 Identity and Services	40.0
MICROMS101 – Microsoft 365 Mobility and Security	40.0
PROGRAM TOTAL	**80.0**

Microsoft 365 Identity and Services

Exam # Reference: MS-100

Course Objectives

This course covers three central elements of Microsoft 365 enterprise administration – Microsoft 365 tenant and service management, Office 365 management, and Microsoft 365 identity management.

After completing this course, students will be able to:

- Designing, configuring, and managing your Microsoft 365 tenant
- Office 365 product functionality
- Configuring Office 365
- Managing Office 365 ProPlus deployments
- Planning and implementing identity synchronization
- Implementing application and external access

Course Outline

Module 1: Designing Your Microsoft 365 Tenant

Lessons

- Planning Microsoft 365 in your On-premises Infrastructure
- Planning Your Identity and Authentication Solution
- Planning Your Service Setup
- Planning Your Hybrid Environment
- Planning Your Migration to Office 365

Module 2: Configuring Your Microsoft 365 Tenant

Lessons

- Planning Your Microsoft 365 Experience
- Configuring Your Microsoft 365 Experience
- Managing User Accounts and Licenses in Microsoft 365
- Managing Security Groups in Microsoft 365
- Implementing Your Domain Services
- Leveraging FastTrack and Partner Services

Module 3: Lab 1 - Configuring your Microsoft 365 Tenant

Lab: Configuring your Microsoft 365 Tenant

- Exercise 1 - Set up a Microsoft 365 Trial Tenant

Module 4: Managing Your Microsoft 365 Tenant

Lessons

- Configuring Tenant Roles
- Managing Tenant Health and Services

Module 5: Lab 2 - Managing your Microsoft 365 Tenant

Lab : Managing your Microsoft 365 Tenant

- Exercise 1 - Manage Administration Delegation
- Exercise 2 - Configure Office 365 Message Encryption (OME)
- Exercise 3 - Monitor and Troubleshoot Office 365

Module 6: Office 365 Overview

Lessons

- Exchange Online Overview
- SharePoint Online Overview
- Teams Overview
- Additional Resources Overview
- Device Management Overview

Module 7: Lab 3 - Office 365 Overview

Lab: Office 365 Overview

- Exercise 1 - Exchange Online Overview
- Exercise 2 - SharePoint Online Overview
- Exercise 3 - Teams Overview

Module 8: Configuring Office 365
Lessons
- Office 365 Client Overview
- Configuring Office Client Connectivity to Office 365

Module 9: Managing Office 365 ProPlus Deployments
Lessons
- Managing User-Driven Client Installations
- Managing Centralized Office 365 ProPlus Deployments
- Configuring Office Telemetry
- Configuring Microsoft Analytics

Module 10: Lab 4 - Managing Office 365 ProPlus installations
Lab: Managing Office 365 ProPlus installations
- Exercise 1 - Prepare an Office 365 ProPlus Managed Installation
- Exercise 2 - Manage a Centralized Office 365 ProPlus Installation
- Exercise 3 - Deploy and Configure Office Telemetry Components

Module 11: Planning and Implementing Identity Synchronization
Lessons
- Introduction to Identity Synchronization
- Planning for Azure AD Connect
- Implementing Azure AD Connect
- Managing Synchronized Identities
- Password Management in Microsoft 365

Module 12: Lab 5 - Implementing Identity Synchronization
Lab: Implementing Identity Synchronization
- Exercise 1 - Set up your organization for identity synchronization
- Exercise 2 - Implement Identity Synchronization

Module 13: Implementing Application and External Access
Lessons
- Implementing Applications in Azure AD
- Configuring Azure AD App Proxy
- Designing Solutions for External Access

Microsoft 365 Mobility and Security

Exam # Reference: MS-101

Course Objectives

This course covers three central elements of Microsoft 365 enterprise administration – Microsoft 365 security management, Microsoft 365 compliance management, and Microsoft 365 device management.

After completing this course, students will be able to:

- Microsoft 365 Security Metrics
- Microsoft 365 Security Services
- Microsoft 365 Threat Intelligence
- Data Governance in Microsoft 365
- Archiving and Retention in Office 365
- Data Governance in Microsoft 365 Intelligence
- Search and Investigations
- Device Management
- Windows 10 Deployment Strategies
- Mobile Device Management

Module 1: Introduction to Microsoft 365 Security Metrics

Lessons

- Threat Vectors and Data Breaches
- Security Solutions in Microsoft 365
- Introduction to the Secure Score
- Introduction to Azure Active Directory Identity Protection

Module 2: Managing Your Microsoft 365 Security Services

Lessons

- Introduction to Exchange Online Protection
- Introduction to Advanced Threat Protection
- Managing Safe Attachments
- Managing Safe Links
- Monitoring and Reports

Module 3: Lab 1 - Manage Microsoft 365 Security Services

Lab: Manage Microsoft 365 Security Services

- Exercise 1 - Set up a Microsoft 365 Trial Tenant
- Exercise 2 - Implement an ATP Safe Links policy and Safe Attachment policy

Module 4: Microsoft 365 Threat Intelligence

Lessons

- Overview of Microsoft 365 Threat Intelligence
- Using the Security Dashboard
- Configuring Advanced Threat Analytics

- Implementing Your Cloud Application Security

Module 5: Lab 2 - Implement Alert Notifications Using the Security Dashboard

Lab: Implement Alert Notifications Using the Security Dashboard

- Exercise 1 - Prepare for implementing Alert Policies
- Exercise 2 - Implement Security Alert Notifications
- Exercise 3 - Implement Group Alerts
- Exercise 4 - Implement eDiscovery Alerts

Module 6: Introduction to Data Governance in Microsoft 365

Lessons

- Introduction to Archiving in Microsoft 365
- Introduction to Retention in Microsoft 365
- Introduction to Information Rights Management
- Introduction to Secure Multipurpose Internet Mail Extension
- Introduction to Office 365 Message Encryption
- Introduction to Data Loss Prevention

Module 7: Archiving and Retention in Office 365

Lessons

- In-Place Records Management in SharePoint
- Archiving and Retention in Exchange
- Retention Policies in the SCC

Module 8: Lab 3 - Implement Archiving and Retention

Lab: Implement Archiving and Retention

- Exercise 1 - Initialize Compliance in Your Organization
- Exercise 2 - Configure Retention Tags and Policies
- Exercise 3 - Implement Retention Policies

Module 9: Implementing Data Governance in Microsoft 365 Intelligence

Lessons

- Planning Your Security and Compliance Needs
- Building Ethical Walls in Exchange Online
- Creating a Simple DLP Policy from a Built-in Template
- Creating a Custom DLP Policy
- Creating a DLP Policy to Protect Documents
- Working with Policy Tips

Module 10: Lab 4 - Implement DLP Policies

Lab: Implement DLP Policies

- Exercise 1 - Manage DLP Policies
- Exercise 2 - Test MRM and DLP Policies

Module 11: Managing Data Governance in Microsoft 365
Lessons

- Managing Retention in Email
- Troubleshooting Data Governance
- Implementing Azure Information Protection
- Implementing Advanced Features of AIP
- Implementing Windows Information Protection

Module 12: Lab 5 - Implement AIP and WIP
Lab: Implement AIP and WIP

- Exercise 1 - Implement Azure Information Protection
- Exercise 2 - Implement Windows Information Protection

Module 13: Managing Search and Investigations
Lessons

- Searching for Content in the Security and Compliance Center
- Auditing Log Investigations
- Managing Advanced eDiscovery

Module 14: Lab 6 - Manage Search and Investigations
Lab: Manage Search and Investigations

- Exercise 1 - Investigate Your Microsoft 365 Data
- Exercise 2 - Configure and Deploy a Data Subject Request

Module 15: Planning for Device Management
Lessons

- Introduction to Co-management
- Preparing Your Windows 10 Devices for Co-management
- Transitioning from Configuration Manager to Intune
- Introduction to Microsoft Store for Business
- Planning for Mobile Application Management

Module 16: Lab 7 - Implement the Microsoft Store for Business
Lab: Implement the Microsoft Store for Business

- Exercise 1 - Configure the Microsoft Store for Business
- Exercise 2 - Manage the Microsoft Store for Business

Module 17: Planning Your Windows 10 Deployment Strategy
Lessons

- Windows 10 Deployment Scenarios
- Implementing Windows Autopilot
- Planning Your Windows 10 Subscription Activation Strategy

- Resolving Windows 10 Upgrade Errors
- Introduction to Windows Analytics

Module 18: Implementing Mobile Device Management
Lessons

- Planning Mobile Device Management
- Deploying Mobile Device Management
- Enrolling Devices to MDM
- Managing Device Compliance

Module 19: Lab 8 - Manage Devices with Intune
Lab: Manage Devices with Intune

- Exercise 1 - Enable Device Management
- Exercise 2 - Configure Azure AD for Intune
- Exercise 3 - Create Intune Policies
- Exercise 4 - Enroll a Windows 10 Device

Preparation for ITIL Foundations

Distance Learning (Online) and Fort Walton Beach

The purpose of the ITIL Foundation certificate in IT Service Management is to certify that the candidate has gained knowledge of the ITIL terminology, structure and basic concepts and has comprehended the core principles of ITIL practices for Service Management.

Program Objective:
To prepare to obtain the ITIL Foundations certification.

Program Requirements:
A typical student should have some basic computer knowledge, but computer knowledge or experience is not required.

- The target group of the ITIL Foundation certificate in IT Service Management is drawn from:
  - Individuals who require a basic understanding of the ITIL framework and how it may be used to enhance the quality of IT service management within an organization.
  - IT professionals that are working within an organization that has adopted and adapted ITIL who need to be informed about and thereafter contribute to an ongoing service improvement program.
  - This may include but is not limited to, IT professionals, business managers and business process owners.

COURSE TITLE	**CLOCK HOURS**
ITIL0001 – ITIL Foundations	36
PROGRAM TOTAL	**36.0**

ITIL 4 Foundations

Exam # Reference: ITIL Foundations v4

Course Objectives:
The **ITIL 4 - Foundation** course provides IT leaders, management, and support staff with a comprehensive introduction to the core concepts of ITIL 4. It is designed to equip students with a practical understanding of ITIL 4 key concepts, principles, and practices that enable modern IT-enabled services in today's digital economy.

This course is based on the latest ITIL 4 best-practice guidance and will prepare the attendee for the ITIL 4 Foundation exam normally given at its conclusion. Candidates who wish to acquire knowledge in the theory and practices of the ITIL 4 management framework. This knowledge is also required if the candidate wishes to pursue any of the ITIL 4 certification schemes.

Upon completion of this course, students will be able to do the following:

- Understand how project management effects business
- Create a charter
- Identify stakeholders
- Create a project management plan
- Create a schedule
- Create a budget
- Create a risk register
- Create various management plans
- Analyze project risks
- Address project related procurement and monitor and control it as needed
- How to close the project, including project and contract closeout.

Course Outline

1 - Framework

- Projects, Programs and Portfolios
- Processes, Knowledge Areas and Process Groups
- Roles and Responsibilities
- Organizational Structures

2 - Integration

- Develop Project Charter
- Develop Project Management Plan
- Direct and Manage Project Execution
- Monitor and Control Project Work
- Perform Integrated Change Control
- Close Project or Phase

3 - Scope

- Plan Scope Management
- Collect Requirements
- Define Scope
- Create WBS
- Validate Scope
- Control Scope

4 - Time

- Plan Schedule Management
- Define Activities
- Sequence Activities
- Estimate Activity Resources

- Estimate Activity Durations
- Develop Schedule
- Network Diagram Exercises
- Control Schedule

5 - Cost
- Plan Cost Management
- Estimate Costs
- Determine Budget
- Control Costs
- Earned Value Exercises

6 - Quality
- Plan Quality Management
- Perform Quality Assurance
- Control Quality

7 – Human Resources
- Plan Human Resource Management
- Acquire Project Team
- Develop Project Team
- Manage Project Team

8 - Communications
- Plan Communications Management
- Manage Communications
- Control Communications

9 - Risk
- Plan Risk Management
- Identify Risks
- Perform Qualitative Risk Analysis
- Perform Quantitative Risk Analysis
- Plan Risk Responses
- Control Risks

10 - Procurement
- Plan Procurement Management
- Conduct Procurements
- Control Procurements

- Close Procurements

11 - Stakeholder

- Identify Stakeholders
- Plan Stakeholder Management
- Manage Stakeholder Engagement
- Control Stakeholder Engagement

12 – Professional and Social Responsibility (PMP)® Only

- Responsibility of a Project Manager
- Respect as a Project Manager
- Fairness in Project Management
- Honesty as a Project Manager

13 – Course Wrap Up

Preparation for Project Management and Six Sigma Professional

Distance Learning (Online) and Fort Walton Beach

This program is designed to provide a student with the skills needed to be a successful project manager in today's rapidly changing world. Students will be equipped as project professionals to apply recognized practices of project management and to understand a project's life cycle, roles, and necessary skill to effectively initiate, plan, execute, monitor, control and close a project. The PMP credential demonstrates to employers, clients and colleagues that a project manager possesses project management knowledge, experience and skills to bring projects to successful completion. The PMP recognizes the competence of an individual to perform in the role of a project manager, specifically experience in leading and directing projects. Finally, the addition of the Six Sigma Green Belt training will demonstrate the student's ability to analyze and solve quality problems to prepare them to be involved in quality improvement projects.

Program Objective:
To prepare to obtain the CompTIA Project+, the Project Management Professional (PMP) & the Certified Six Sigma Green Belt (CSSGB) certifications.

Program Requirements:

Education Experience / Project Management Experience:
1. Secondary degree (High School Diploma, Associates degree or global equivalent)
2. Minimum five years/60 months unique non-overlapping professional project management experience during which at least 7,500 hours were spent leading and directing project tasks
OR
3. Four-year degree (Bachelor's degree or global equivalent)
4. Minimum three years/36 months unique non-overlapping professional project management experience during which at least 4,500 hours were spent leading and directing project tasks

COURSE TITLE	CLOCK HOURS
COMPT007 – CompTIA Project+ Certification	40
SSGB1000 – Certified Six Sigma Green Belt (CSSGB) Certification	32.5
PMP1000 – Project Management Professional (PMP) Certification	32.5
PROGRAM TOTAL	**105.0**

CompTIA Project+

Exam # Reference: PK0-0041

Course Overview

The Project+ course is designed to help students master the skills needed to be a successful project manager. Students can expect to gain knowledge on recognized practices of project management, a project's life cycle, roles, and skills necessary to effectively initiate, plan, execute, monitor, control and close a project. The course focus point is learning the ability to initiate, manage and support a project or business initiative. Working through case studies with real-world scenarios, you will interact with fellow students to learn and apply the methodologies and good practices of formal project management.

Upon completion of this course, students will be able to do the following:

- Identify the fundamentals of project management.
- Initiate a project.
- Create project plans, stakeholder strategies, and scope statement.
- Develop a Work Breakdown Structure and activity lists.
- Develop project schedule and identify the critical path.
- Plan project costs.
- Create project staffing and quality management plans.
- Create an effective communication plan.
- Create a risk management plan, perform risk analysis, and develop a risk response plan.
- Plan project procurements.
- Develop change management and transition plans.
- Assemble and launch the project team to execute the plan.
- Execute the project procurement plan.
- Monitor and control project performance.
- Monitor and control project constraints.
- Monitor and control project risks.
- Monitor and control procurements.
- Perform project closure activities.

Course Outline

1 - DEFINING PROJECT MANAGEMENT FUNDAMENTALS

- Identify Project Management Basics
- Describe the Project Life Cycle
- Identify Organizational Influences on Project Management
- Define Agile Methodology

2 - INITIATING THE PROJECT

- Identify the Project Selection Process
- Prepare a Project SOW
- Create a Project Charter
- Identify Project Stakeholders

3 - PLANNING THE PROJECT

- Identify Project Management Plan Components
- Determine Stakeholder Needs
- Create a Scope Statement

4 - PREPARING TO DEVELOP THE PROJECT SCHEDULE

- Develop a WBS
- Create an Activity List
- Identify the Relationships Between Activities
- Identify Resources
- Estimate Time

5 - DEVELOPING THE PROJECT SCHEDULE

- Develop a Project Schedule
- Identify the Critical Path
- Optimize the Project Schedule
- Create a Schedule Baseline

6 - PLANNING PROJECT COSTS

- Estimate Project Costs
- Estimate the Cost Baseline
- Reconcile Funding and Costs

7 - PLANNING HUMAN RESOURCES AND QUALITY MANAGEMENT

- Create a Human Resource Plan
- Create a Quality Management Plan

8 - COMMUNICATING DURING THE PROJECT

- Identify Communication Methods
- Create a Communications Management Plan

9 - PLANNING FOR RISK

- Create a Risk Management Plan
- Identify Project Risks and Triggers
- Perform Qualitative Risk Analysis

- Perform Quantitative Risk Analysis
- Develop a Risk Response Plan

10 - PLANNING PROJECT PROCUREMENTS

- Collect Project Procurement Inputs
- Prepare a Procurement Management Plan
- Prepare Procurement Documents

11 - PLANNING FOR CHANGE AND TRANSITIONS

- Develop an Integrated Change Control System
- Develop a Transition Plan

12 - EXECUTING THE PROJECT

- Direct the Project Execution
- Execute a Quality Assurance Plan
- Assemble the Project Team
- Develop the Project Team
- Manage the Project Team
- Distribute Project Information
- Manage Stakeholder Relationships and Expectations

13 - EXECUTING THE PROCUREMENT PLAN

- Obtain Responses from Vendors
- Select Project Vendors

14 - MONITORING AND CONTROLLING PROJECT PERFORMANCE

- Monitor and Control Project Work
- Manage Project Changes
- Report Project Performance

15 - MONITORING AND CONTROLLING PROJECT CONSTRAINTS

- Control Project Scope
- Control Project Schedule
- Control Project Costs
- Manage Project Quality

16 - MONITORING AND CONTROLLING PROJECT RISKS

- Monitor and Control Project Risks

17 - MONITORING AND CONTROLLING PROCUREMENTS

- Monitor and Control Vendors and Procurements

- Handling Legal Issues

18 - CLOSING THE PROJECT

- Deliver the Final Product
- Close Project Procurements
- Close a Project

Lean Six Sigma Green Belt

Exam # Reference: CSSGB

Course Overview

The Lean Six Sigma Green Belt course aims to prepare students to perform the role of a Lean Six Sigma Green Belt. The comprehensive curriculum covers everything within the Lean Six Sigma D-M-A-I-C body of knowledge and the problem-solving strategy is demonstrated throughout the course. Various Statistical and Business Improvement tools help students to understand the flow and process of the methodology.

At the completion of this course, participants will be able to do the following:

- Understand the concept of Six Sigma and the DMAIC approach to process improvement
- Understand the tools involved in the Define, Measure, Analyze, Improve and Control phases
- Understand the use of the tools in characterizing processes, analyzing process data, solving problems and controlling processes
- Use the key tools to solve practical business problems
- Lead small Six Sigma project teams or assist Black Belts to deliver tangible business results on larger projects

Course Outline

Define Phase

- Understanding Six Sigma
- Six Sigma Fundamentals
- Selecting Projects
- Elements of Waste
- Conclusion and Action Items

Measure Phase

- Introduction to Measure
- Process Discovery
- Six Stigma Statistics

- Measurement System Analysis
- Process Capability
- Conclusion and Action Items

Analyze Phase

- Introduction to Analyze
- "X" Sifting
- Inferential Statistics
- Introduction to Hypothesis Testing
- Hypothesis Testing Normal Data Part 1 & 2
- Hypothesis Testing Non-Normal Data Part 1 & 2
- Conclusion and Action Items

Improve Phase

- Introduction to Improve
- Process Modeling Progression
- Advanced Process Modeling
- Experimental Design
- Conclusion and Action Items

Control Phase

- Introduction to Control
- Lean Controls
- Defect Controls
- Statistical Process Control (SPC)
- Six Sigma Control Plans
- Conclusion and Action Items

Project Management Professional (PMP)

Exam # Reference: PMP

Course Overview

This course is for students who have on the job experience doing project management activities and running projects, regardless of their job title. It is for students who wish to become certified project managers, or those that want to build or reinforce a foundation in project management. This course is ideal for students who want to grow and formalize their project management skills on an industry neutral, global standard This course is ideal for a leader or manager wanting to take their career and salary to the next level in earning a globally recognized credential (PMP)®.

Upon successful completion of this course, students will be able to do the following:

- Understand how project management effects business
- Create a charter
- Identify stakeholders
- Create a project management plan
- Create a schedule
- Create a budget
- Create a risk register
- Create various management plans
- Analyze project risks
- Address project related procurement and monitor and control it as needed
- How to close the project, including project and contract closeout.

Course Outline

1 - FRAMEWORK

- Projects, Programs and Portfolios
- Processes, Knowledge Areas and Process Groups
- Roles and Responsibilities
- Organizational Structures

2 - INTEGRATION

- Develop Project Charter
- Develop Project Management Plan
- Direct and Manage Project Execution
- Monitor and Control Project Work
- Perform Integrated Change Control
- Close Project or Phase

3 - SCOPE

- Plan Scope Management
- Collect Requirements
- Define Scope
- Create WBS
- Validate Scope
- Control Scope

4 - TIME

- Plan Schedule Management

- Define Activities
- Sequence Activities
- Estimate Activity Resources
- Estimate Activity Durations
- Develop Schedule
- Network Diagram Exercises
- Control Schedule

5 - COST

- Plan Cost Management
- Estimate Costs
- Determine Budget
- Control Costs
- Earned Value Exercises

6 - QUALITY

- Plan Quality Management
- Perform Quality Assurance
- Control Quality

7 - HUMAN RESOURCE

- Plan Human Resource Management
- Acquire Project Team
- Develop Project Team
- Manage Project Team

8 - COMMUNICATIONS

- Plan Communications Management
- Manage Communications
- Control Communications

9 - RISK

- Plan Risk Management
- Identify Risks
- Perform Qualitative Risk Analysis
- Perform Quantitative Risk Analysis
- Plan Risk Responses
- Control Risks

10 - PROCUREMENT

- Plan Procurement Management

- Conduct Procurements
- Control Procurements
- Close Procurements

11 - STAKEHOLDER

- Identify Stakeholders
- Plan Stakeholder Management
- Manage Stakeholder Engagement
- Control Stakeholder Engagement

12 - PROFESSIONAL AND SOCIAL RESPONSIBILITY (PMP)® ONLY

- Responsibility of a Project Manager
- Respect as a Project Manager
- Fairness in Project Management
- Honesty as a Project Manager

13 - COURSE WRAP-UP

Preparation for Six Sigma Green Belt Professional

Distance Learning (Online) and Fort Walton Beach

The Six Sigma Green Belt operates in support of or under the supervision of a Six Sigma Black Belt and analyzes and solves quality problems and is involved in quality improvement projects. This program is designed to give the student a solid understanding of Six Sigma principles and teach you how to effectively work within a Six Sigma team. You will learn to improve quality and reduce defects within your organization.

Program Objective:
To prepare to obtain the Certified Six Sigma Green Belt (CSSGB) certification.

Program Requirements:
Secondary degree (High School Diploma, Associates degree or global equivalent.) A few years of work experience with process improvement teams is helpful but not required.

COURSE TITLE	CLOCK HOURS
SSGB 1000 – Certified Six Sigma Green Belt (CSSGB) Certification	32.5
PROGRAM TOTAL	**32.5**

Lean Six Sigma Green Belt

Exam # Reference: CSSGB

Course Overview

The Lean Six Sigma Green Belt course aims to prepare students to perform the role of a Lean Six Sigma Green Belt. The comprehensive curriculum covers everything within the Lean Six Sigma D-M-A-I-C body of knowledge and the problem-solving strategy is demonstrated throughout the course. Various Statistical and Business Improvement tools help students to understand the flow and process of the methodology.

At the completion of this course, participants will be able to do the following:

- Understand the concept of Six Sigma and the DMAIC approach to process improvement
- Understand the tools involved in the Define, Measure, Analyze, Improve and Control phases
- Understand the use of the tools in characterizing processes, analyzing process data, solving problems and controlling processes
- Use the key tools to solve practical business problems
- Lead small Six Sigma project teams or assist Black Belts to deliver tangible business results on larger projects

Course Outline

Define Phase

- Understanding Six Sigma
- Six Sigma Fundamentals
- Selecting Projects
- Elements of Waste
- Conclusion and Action Items

Measure Phase

- Introduction to Measure
- Process Discovery
- Six Stigma Statistics
- Measurement System Analysis
- Process Capability
- Conclusion and Action Items

Analyze Phase

- Introduction to Analyze
- "X" Sifting
- Inferential Statistics
- Introduction to Hypothesis Testing
- Hypothesis Testing Normal Data Part 1 & 2
- Hypothesis Testing Non-Normal Data Part 1 & 2
- Conclusion and Action Items

Improve Phase

- Introduction to Improve
- Process Modeling Progression
- Advanced Process Modeling
- Experimental Design
- Conclusion and Action Items

Control Phase

- Introduction to Control
- Lean Controls
- Defect Controls
- Statistical Process Control (SPC)
- Six Sigma Control Plans
- Conclusion and Action Items

Preparation for Adobe Certified Associate – To be removed

Distance Learning (Online) and Fort Walton Beach

The Adobe Certified Associate is an industry-recognized credential that demonstrates proficiency in Adobe digital skills. Whether you're just starting out in your career, looking to switch jobs or interested in preparing for success in the job market, the Adobe Certified Associate program is for you. This program will equip and prepare students to achieve the Adobe Certified Associate certification for three Adobe Creative Cloud software specialties: Illustrator, Photoshop and InDesign.

- Adobe Certified Associate (ACE) – Illustrator
- Adobe Certified Associate (ACE) – InDesign
- Adobe Certified Associate (ACA) - Photoshop

Program Objective:
To prepare to obtain the Adobe Certified Associate (ACA) – Illustrator, Adobe Certified Associate (ACA) – InDesign and Adobe Certified Associate (ACA) - Photoshop certifications.

Program Requirements:
Secondary degree (High School Diploma, Associates degree or global equivalent.) One year of general computing experience is recommended.

COURSE TITLE	CLOCK HOURS
ADOBE020 – Adobe Illustrator	40
ADOBE021 – Adobe InDesign	40
ADOBE022 – Adobe Photoshop	40
PROGRAM TOTAL	**120.0**

Adobe Illustrator

Exam # Reference: Adobe Certified Associate (ACA) Adobe Certified Expert (ACE)

Course Overview
This course is designed to teach the key fundamentals for working in Illustrator. Students will learn techniques through hands-on projects to create logos, illustrations, posters and more. It will help to build a strong foundation from exacting illustration to free-form painting.

Upon successful completion of this course, students will be able to do the following:

- Navigate the Illustrator interface.
- Create an illustration.
- Draw and edit shapes.
- Work with layers.

- Customize artwork with drawing tools and effects.

Course Outline

1 – GETTING TO KNOW THE WORK AREA

- Starting Illustrator and opening a file
- Exploring the workspace
- Changing the view of artwork
- Navigating artboards
- Arranging multiple documents

2 – TECHNIQUES FOR SELECTING ARTWORK

- Selecting objects
- Aligning objects
- Working with groups
- Exploring object arrangement

3 – USING SHAPES TO CREAT ARTWORK FOR A POSTCARD

- Creating a new document
- Working with basic shapes
- Working with the Shaper tool
- Using Image Trace
- Working with drawing modes

4 – EDITING AND COMBINING SHAPES AND PATHS

- Editing paths and shapes
- Using the Eraser tool
- Combining shapes
- Using the width tool

5 – TRANSFORMING ARTWORK

- Working with artboards
- Working with rulers and guides
- Transforming content

6 – CREATING AN ILLUSTRATION WITH THE DRAWING TOOLS

- An intro to drawing with the Pen tool
- Creating artwork with the Pen tool

- Drawing with the Curvature tool
- Editing curves
- Creating a dashed line
- Adding arrowheads to a path
- Working with the Pencil tool
- Joining with the Join tool

7 – USING COLOR TO ENHANCE SIGNAGE

- Exploring color modes
- Working with color
- Working with Live Paint

8 – ADDING TYPE TO A POSTER

- Adding type
- Formatting type
- Fixing missing fonts
- Resizing and reshaping type objects
- Creating and applying test styles
- Wrapping text
- Warping text
- Working with type on a path
- Creating text outlines

9 – ORGANIZING YOUR ARTWORK WITH LAYERS

- Creating layers and sublayers
- Editing layers and objects
- Duplicating layer content
- Creating a clipping mask

10 – GRADIENTS, BLENDS, AND PATTERNS

- Working with gradients
- Working with blended objects
- Painting with patterns

11 – USING BRUSHES TO CREATE A POSTER

- Working with brushes
- Using Calligraphic brushes
- Removing a brush stroke

- Using Art brushes
- Using Bristle brushes
- Using Pattern brushes
- Working with the Blob Brush tool

12 – EXPLORING CREATIVE USES OF EFFECTS AND GRAPHIC STYLES

- About camera raw files
- Processing files in Camera Raw
- Applying advanced color correction

13 – CREATING ARTWORK FOR A T-SHIRT

- Using the Appearance panel
- Using live effects
- Applying a Photoshop effect
- Using graphic styles
- Applying a graphic style to a layer

14 – USING ILLUSTRATOR CC WITH OTHER ABODE APPLICATIONS

- Combining artwork
- Placing image files
- Masking images
- Working with image links
- Packaging a file
- Creating a PDF

15 – EXPORTING ASSETS

- Creating Pixel-Perfect Drawings
- Exporting artboards and assets
- Creating CSS from your design

Course Overview

This course is designed to train beginning Adobe InDesign users the fundamental features of the program as well as elevate their skills, understand best practices, and learn about new features. It will show users the key techniques for working in InDesign. Students will build a strong foundation of typographic, page layout, and document-construction skills that will enable them to produce a broad range of print and digital publications.

Upon successful completion of this course, students will be able to do the following:

- Navigate the InDesign interface.
- Create a new document.
- Customize a document using color, swatches, gradients, and styles.
- Manage page elements.
- Add tables.
- Prepare documents for digital or print deployment.

Course Outline

1 - INTRODUCING THE WORKSPACE

- Looking at the workspace
- Working with panels
- Customizing the workspace
- Navigating through a document
- Using context menus
- Using panel menus
- Modifying interface preferences

2 - GETTING TO KNOW INDESIGN

- Viewing guides
- Preflighting as you work
- Adding text
- Working with styles
- Working with graphics
- Working with objects
- Working with object styles
- Viewing the document in Presentation mode

3 - SETTING UP A DOCUMENT AND WORKING WITH PAGES

- Creating and saving custom document settings
- Creating a new document
- Switching between open InDesign documents
- Working with master pages
- Applying master pages to document pages
- Adding new document pages
- Rearranging and deleting document pages
- Changing the size of pages
- Adding sections to change page numbering
- Overriding master page items and placing text and graphics
- Printing to the edge of the paper: using the bleed guides
- Viewing the completed spread

4 - WORKING WITH OBJECTS

- Working with layers
- Creating and modifying text frames
- Creating and modifying graphics frames
- Adding metadata captions to graphics frames
- Placing and linking graphics frames
- Changing the shape of a frame
- Wrapping text around a graphic
- Modifying the shape of frames
- Transforming and aligning objects
- Selecting and modifying grouped objects
- Drawing lines and modifying arrowheads
- Creating a QR code

5 - FLOWING TEXT

- Flowing text into an existing frame
- Flowing text manually
- Creating text frames while flowing text
- Creating threaded frames automatically
- Flowing text automatically
- Applying paragraph styles to text
- Adjusting columns

6 - EDITING TEXT

- Finding and changing a missing font

- Entering and importing text
- Finding and changing text and formatting
- Checking spelling
- Editing text by dragging and dropping
- Using the Story Editor
- Tracking changes

7 - WORKING WITH TYPOGRAPHY

- Adjusting vertical spacing
- Working with fonts, type styles, and glyphs
- Fine-tuning columns
- Changing paragraph alignment
- Creating a drop cap
- Adjusting letter and word spacing
- Adjusting line breaks
- Setting tabs
- Adding a rule above a paragraph
- Working with paragraph shading

8 - WORKING WITH COLOR

- Managing color
- Defining printing requirements
- Creating colors
- Applying colors
- Working with tint swatches
- Working with gradients
- Working with color groups

9 - WORKING WITH STYLES

- Creating and applying paragraph styles
- Creating and applying character styles
- Nesting character styles inside paragraph styles
- Creating and applying object styles
- Creating and applying table and cell styles
- Globally updating styles

- Loading styles from another document

10 - IMPORTING AND MODIFYING GRAPHICS

- Adding graphics from other programs
- Comparing vector and bitmap graphics
- Managing links to imported files
- Updating revised graphics
- Adjusting display quality
- Working with dropped backgrounds
- Working with alpha channels
- Importing native Adobe graphic files
- Using an InDesign library to manage objects
- Using Adobe Bridge to import graphics

11 - CREATING TABLES

- Creating a table
- Converting text to a table
- Changing rows and columns
- Formatting a table
- Adding graphics to table cells
- Creating a header row
- Creating and applying table and cell styles

12 - WORKING WITH TRANSPARENCY

- Importing and colorizing a grayscale image
- Applying transparency settings
- Adding transparency effects to imported vector and bitmap graphics
- Importing and adjusting Illustrator files that use transparency
- Applying transparency settings to text
- Working with effects

13 - PRINTING AND EXPORTING

- Managing colors
- Previewing transparency effects

- Previewing the page
- Creating an Adobe PDF proof
- Creating a Press-Ready PDF and saving a PDF preset
- Printing a proof and saving a print preset
- Packaging files

14 - CREATING ADOBE PDF FILES WITH FORM FIELDS

- Set up a workspace for forms
- Adding form fields
- Setting the tab order of the fields
- Adding a button to submit the form
- Exporting an interactive Adobe PDF file
- Testing your form in Adobe Acrobat Reader

15 - CREATING A FIXED-LAYOUT EPUB

- Creating a new document for fixed-layout export
- EPUB: reflowable versus fixed-layout
- Adding animation
- Buttons
- Adding multimedia and interactive elements
- Exporting an EPUB file

Adobe Photoshop CC

Exam # Reference: Adobe Certified Associate (ACA) Visual Design Using Adobe Photoshop, or Certified Expert (ACE) Photoshop CC

Course Overview

This course is designed to teach the essential elements of the Photoshop interface. Students will learn techniques for working in Photoshop, including how to correct, enhance, and distort digital images, create image composites, and prepare images for print and the web.

Upon successful completion of this course, students will be able to do the following:

- Navigate the InDesign interface.
- Create a new document.
- Customize a document using color, swatches, gradients, and styles.
- Manage page elements.

- Add tables.
- Prepare documents for deployment.

Course Outline

1 – GETTING TO KNOW THE WORK AREA

- Starting to work in Adobe Photoshop
- Using the tools
- Sampling a color
- Working with the tools and tool properties
- Undoing actions in Photoshop
- More about panels and panel locations

2 – BASIC PHOTO CORRECTIONS

- Strategy for retouching
- Resolution and image size
- Opening a file with Adobe Bridge
- Straightening and cropping the image in Photoshop
- Adjusting the color and tone
- Using the Spot Healing Brush tool
- Applying a content-aware patch
- Repairing areas with the Clone Stamp tool
- Sharpening the image

3 – WORKING WITH SELECTIONS

- About selecting and selection tools
- Using the Quick Selection tool
- Moving a selected area
- Manipulating selections
- Using the Magic Wand tool
- Selecting with the lasso tools
- Rotating a selection
- Selecting with the Magnetic Lasso tool
- Selecting from a center point
- Resizing and copying a selection
- Cropping an image

4 – LAYER BASIC

- About layers
- Using the Layers panel
- Rearranging layers
- Applying a gradient to a layer
- Applying a layer style
- Adding an adjustment layer
- Updating layer effects
- Adding a border
- Flattening and saving files

5 – QUICK FIXES

- Improving a snapshot
- Adjusting facial features with Liquify
- Blurring a background
- Creating a panorama
- Filling empty areas when cropping
- Correcting image distortion
- Extending depth of field
- Removing objects using Content-Aware Fill
- Adjusting perspective in an image

6 – MASKS AND CHANNELS

- Working with masks and channels
- Using Select and Mask and Select Subject
  Creating a quick mask
- Manipulating an image with Puppet Warp
- Using an alpha channel to create a shadow

7 – TYPOGRAPHIC DESIGN

- About type
- Creating a clipping mask from type
- Creating type on a path
- Warping point type
- Designing paragraphs of type
- Adding a rounded rectangle
- Adding vertical text

8 – VECTOR DRAWING TECHNIQUES

- About bitmap images and vector graphics
- About paths and the Pen tool
- Drawing with the Pen tool
- Working with defined custom shapes
- Importing a Smart Object
- Adding color and depth to a shape using layer styles

9 – ADVANCED COMPOSITING

- Arranging layers
- Using Smart Filters
- Painting a layer
- Adding a background
- Using the History panel to undo edits
- Upscaling a low-resolution image

10 – PAINTING WITH THE MIXER BRUSH

- About the Mixer Brush
- Selecting brush settings
- Mixing colors
- Mixing colors with a photograph
- Painting and mixing colors with brush presets

11 – EDITING VIDEO

- About the Timeline panel
- Creating a new video project
- Animating text with keyframes
- Creating effects
- Adding transitions
- Adding audio
- Muting unwanted audio

12 – WORKING WITH CAMERA RAW

- About camera raw files
- Processing files in Camera Raw
- Applying advanced color correction

13 – PREPARING FILES FOR THE WEB

- Creating placeholders with the Frame tool

- Using layer groups to create button graphics
- Automating a multistep task
- Designing with artboards

14 – PRODUCING AND PRINTING CONSISTENT COLOR

- Preparing files for printing
- Performing a “zoom test”
- About color management
- Specifying color-management settings
- Identifying out-of-gamut colors
- Proofing document colors on a monitor
- Bringing colors into the output gamut
- Converting an image to CMYK
- Saving the image as a CMYK EPS file
- Printing a CMYK image from Photoshop

15 – PRINTING 3D FILES

- Understanding the 3D environment
- Positioning 3D elements
- Printing a 3D file

PROGRAM TUITION AND FEE PAYMENT SCHEDULES

TUITION AND FEES

Preparation for Secure Infrastructure Specialist

Registration Fee:	$150.00
Books & Materials:	(Included)
Tuition Cost:	$10,335.00
Total Program Cost:	$10,485.00

Preparation for Computer Networking Professional

Registration Fee:	$150.00
Books & Materials:	(Included)
Tuition Cost:	$10,335.00
Total Program Cost:	$10,485.00

Preparation for Computer Network Security Professional

Registration Fee:	$150.00
Books & Materials:	(Included)
Tuition Cost:	$10,335.00
Total Program Cost:	$10,485.00

Preparation for Networking Security and Cloud Technology Professional

Registration Fee:	$150.00
Books & Materials:	(Included)
Tuition Cost:	$17,825.00
Total Program Cost:	$17,975.00

Preparation for Cybersecurity Professional

Registration Fee:	$150.00
Books & Materials:	(Included)
Tuition Cost:	$13,830.00
Total Program Cost:	$13,980.00

Preparation for Advanced Cybersecurity Professional

Registration Fee:	$150.00
Books & Materials:	(Included)
Tuition Cost:	$7,340.00
Total Program Cost:	$7,490.00

Preparation for Linux Network Professional

Registration Fee:	$150.00
Books & Materials:	(Included)
Tuition Cost:	$6,840.00
Total Program Cost:	$6,990.00

Preparation for Python Programming Professional

Registration Fee:	$150.00
Books & Materials:	(Included)
Tuition Cost:	$6,840.00
Total Program Cost:	$6,990.00

Preparation for Cisco Certified Network Administrator

Registration Fee:	$150.00
Books & Materials:	(Included)
Tuition Cost:	$3,845.00
Total Program Cost:	$3,995.00

Preparation for Cisco Certified Network Enterprise Professional

Registration Fee:	$150.00
Books & Materials:	(Included)
Tuition Cost:	$7,340.00
Total Program Cost:	$7,490.00

Preparation for Microsoft Modern Desktop Administrator Associate

Registration Fee:	$150.00
Books & Materials:	(Included)
Tuition Cost:	$6,840.00
Total Program Cost:	$6,990.00

Preparation for Microsoft 365 and Azure Security Administrator Associate

Registration Fee:	$150.00
Books & Materials:	(Included)
Tuition Cost:	$6,840.00
Total Program Cost:	$6,990.00

Preparation for Microsoft Enterprise Administrator Expert

Registration Fee:	$150.00
Books & Materials:	(Included)
Tuition Cost:	$6,840.00
Total Program Cost:	$6,990.00

Preparation for ITIL Foundations

Registration Fee:	$150.00
Books & Materials:	(Included)
Tuition Cost:	$3,345.00
Total Program Cost:	$3,495.00

Preparation for Project Management and Six Sigma Professional Program

Registration Fee:	$150.00
Books & Materials:	(Included)
Tuition Cost:	$10,335.00
Total Program Cost:	$10,485.00

Preparation for Certified Six Sigma Green Belt Professional

Registration Fee:	$150.00
Books & Materials:	(Included)
Tuition Cost:	$3,345.00
Total Program Cost:	$3,495.00

Preparation for Adobe Certified Associate – To be retired

Registration Fee:	$150.00
Books & Materials:	(Included)
Tuition Cost:	$10,335.00
Total Program Cost:	$10,485.00